Intel(R) PROSet/Wireless WiFi Connection Utility User's Guide

Supported WiFi adapters:

- Intel(R) WiMAX/WiFi Link 5350
- Intel(R) WiMAX/WiFi Link 5150
- Intel(R) WiFi Link 5300
- Intel(R) WiFi Link 5100
- Intel(R) Wireless WiFi Link 4965AGN
- Intel(R) Wireless WiFi Link 4965AG_
- Intel(R) PRO/Wireless 3945ABG Network Connection
- Intel(R) PRO/Wireless 2915ABG Network Connection
- Intel(R) PRO/Wireless 2200BG Network Connection

With your wireless network card, you can access wireless networks, share files or printers, or even share your Internet connection. All of these features can be explored using a wireless network in your home or office. This wireless network solution is designed for both home and business use. Additional users and features can be added as your networking needs grow and change.

Depending on the model of your Intel WiFi adapter, your adapter is compatible with 802.11a, 802.11b, 802.11g, and 802.11n wireless standards. Operating at 5 GHz or 2.4 GHz frequency at data rates of up to 300 Mbps, you can now connect your computer to existing high-speed networks that use multiple access points within large or small environments. Your WiFi adapter maintains automatic data rate control according to the access point location and signal strength to achieve the fastest possible connection. All of your wireless network connections are easily managed by the WiFi connection utility. Profiles that are set up through the WiFi connection utility provide enhanced security measures with 802.1X network authentication.

Table of Contents

Information in this document is subject to change without notice.

Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

"IMPORTANT NOTICE FOR ALL USERS OR DISTRIBUTORS:

Intel wireless LAN adapters are engineered, manufactured, tested, and quality checked to ensure that they meet all necessary local and governmental regulatory agency requirements for the regions that they are designated and/or marked to ship into. Because wireless LANs are generally unlicensed devices that share spectrum with radars, satellites, and other licensed and unlicensed devices, it is sometimes necessary to dynamically detect, avoid, and limit usage to avoid interference with these devices. In many instances Intel is required to provide test data to prove regional and local compliance to regional and governmental regulations before certification or approval to use the product is granted. Intel's wireless LAN's EEPROM, firmware, and software driver are designed to carefully control parameters

that affect radio operation and to ensure electromagnetic compliance (EMC). These parameters include, without limitation, RF power, spectrum usage, channel scanning, and human exposure.

For these reasons Intel cannot permit any manipulation by third parties of the software provided in binary format with the wireless LAN adapters (e.g., the EEPROM and firmware). Furthermore, if you use any patches, utilities, or code with the Intel wireless LAN adapters that have been manipulated by an unauthorized party (i.e., patches, utilities, or code (including open source code modifications) which have not been validated by Intel), (i) you will be solely responsible for ensuring the regulatory compliance of the products, (ii) Intel will bear no liability, under any theory of liability for any issues associated with the modified products, including without limitation, claims under the warranty and/or issues arising from regulatory non-compliance, and (iii) Intel will not provide or be required to assist in providing support to any third parties for such modified products.

Note: Many regulatory agencies consider Wireless LAN adapters to be "modules", and accordingly, condition system-level regulatory approval upon receipt and review of test data documenting that the antennas and system configuration do not cause the EMC and radio operation to be non-compliant."

June 2008

Back to Contents

Use the Intel(R) PROSet/Wireless WiFi Connection Utility

Use Intel(R) PROSet/Wireless WiFi Connection Utility as Your Wireless Manager

Intel(R) PROSet/Wireless WiFi Software is used to set up, edit, and manage network profiles to connect to a network. It also includes advanced settings such as power management and channel selection for setting up ad-hoc networks.

If you use Microsoft* Windows XP* Wireless Zero Configuration as your wireless manager, you can disable it from the Microsoft Windows Wireless Network tab.

To disable Microsoft Windows XP Wireless Zero Configuration as your wireless manager:

1. Click **Start > Control Panel**.
2. Double-click **Network Connections**.
3. Right-click **Wireless Network Connection**.
4. Click **Properties**.
5. Click **Wireless Networks**.
6. Verify that the **Use Windows to configure my wireless network settings** is not selected. If it is, clear it.
7. Click **OK**. This confirms that the Intel(R) PROSet/Wireless utility is configured to manage your network profiles.

   NOTE: Verify that the Application Settings option **Notify when another application uses the WiFi adapter** is selected. This option prompts you when Microsoft Windows XP Wireless Zero Configuration starts to manage your network profiles.

Start Intel(R) PROSet/Wireless WiFi Connection Utility

To start the WiFi connection utility, use one of the following methods:

- Click **Start > Programs > Intel PROSet Wireless > WiFi Connection Utility** .
- Right-click the Taskbar icon located in the lower right corner of your Windows Desktop to open the Taskbar menu. Click **Configure WiFi** .
- Double-click the Taskbar icon.

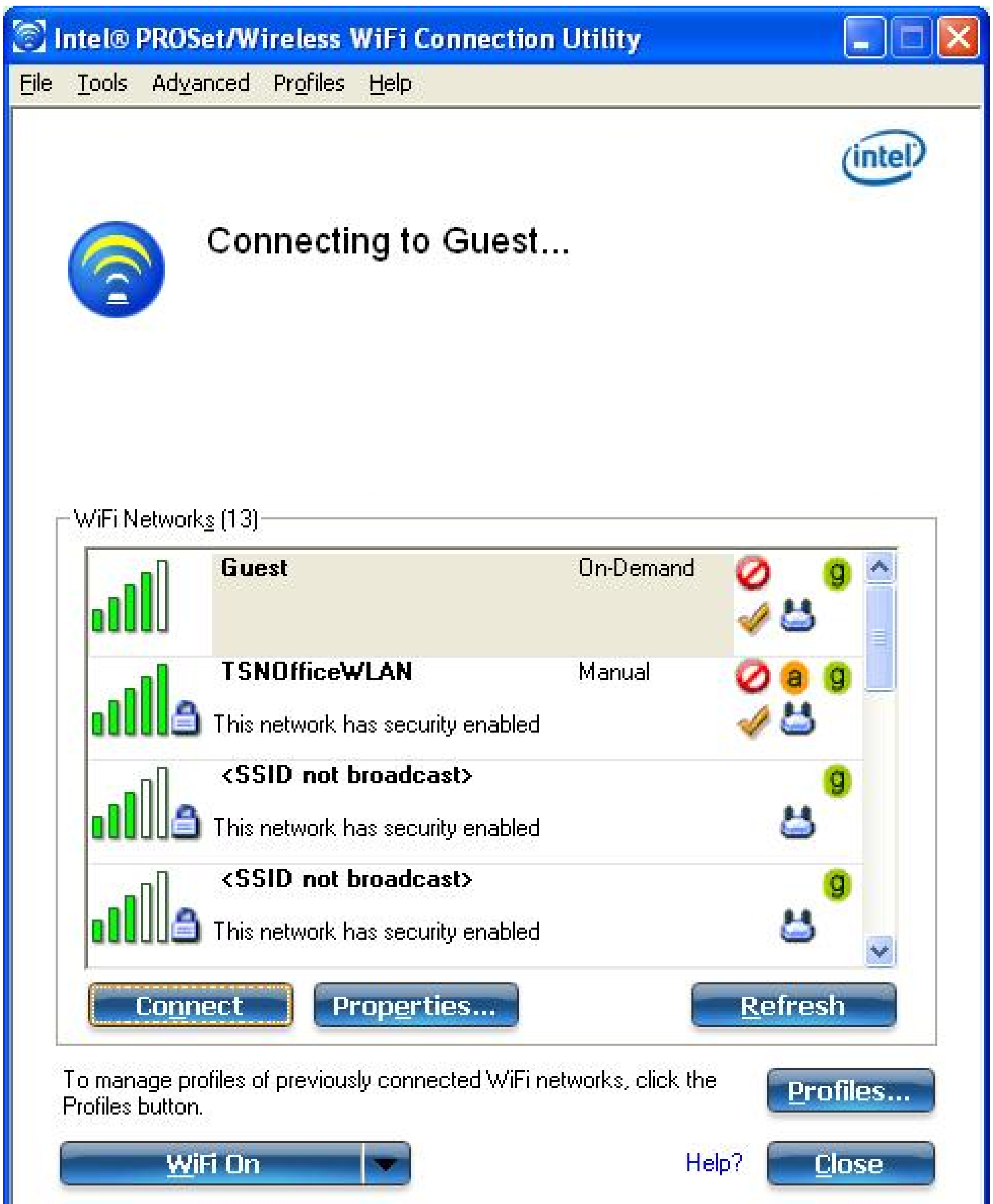
To close the WiFi connection utility from the main window, use one of the following:

- Select **File > Exit** from the main window.
- Click **Close**.
- Click the **Close** button (X) at the top right corner of the window.

Intel(R) PROSet/Wireless WiFi Connection Utility Main Window

The WiFi Connection Utility Main Window lets you:

- View the current connection details (signal quality, speed and current network name).
- Scan for available WiFi networks.
- Manage profiles.
- Auto-connect profiles to available networks in a specific order defined in the Profile list.
- Connect to Infrastructure and Device to Device (ad hoc) networks.
- Configure adapter settings.
- Troubleshoot wireless connection problems.





Connection Details

On the main window, click **Details** to view detailed parameters of the access point and network adapter. The **Connection Details** window displays the current network connection information. See Connection Details for a complete description.

The Taskbar icon also indicates the current connection status. See Taskbar Icons.

Main Window Connection Status Icons

The connection status icons indicate the current connection status of your WiFi adapter. The connection status icon displays in the WiFi connection utility main window See Connection Status Icons.

Profile Management

On the WiFi connection utility main window, click **Connect** on a WiFi network. Once connected, a profile is created in the Profiles list. The Profiles List displays the current user profiles in the order that they are to be applied. Use the up and down arrows to arrange profiles in a specific order to automatically connect to a WiFi network.

You can also add, edit, and remove profiles from the Profiles list. Click Profiles on the WiFi connection utility main window.

Different profiles can be configured for each wireless network. Profile settings can include, the network name (SSID), operating mode, and security settings. See Profile Management for more information.

Menus

Use the **File**, **Tools**, **Advanced**, **Profiles** and **Help** menus to configure your network settings.

Name	Description
File	**Exit**: Closes the WiFi connection utility main window.
Tools	**Application Settings**: Use to set system wide connection preferences. See Application Settings for information. **Intel(R) Wireless Troubleshooter**: Use to resolve wireless network connection problems. See Intel(R) Wireless Troubleshooter for more information. **Manual Diagnostics Tool**: The Manual Diagnostics Tool lets you run a set of diagnostics tests that verify the functionality of your WiFi adapter. See Manual Diagnostics Tool for more information. **Administrator Tool**: Used by administrators or the person who has administrator privileges on this computer to configure shared profiles (Pre-logon/Common, Persistent, and Voice over IP [VoIP]). The Administrator Tool can also be used by an Information Technology department to configure user settings within the WiFi connection utility and to create custom install packages to export to other systems. See Administrator Tool for more information. **NOTE**: The Administrator Tool is available only if it installed during a custom installation of the Intel(R) PROSet/Wireless WiFi Software. See Install Additional Software Features for more information on custom installation.
Advanced	**Adapter Settings**: Displays Adapter Settings that are equivalent to the settings in the Microsoft Windows Advanced settings. See Adapter Settings for information. To access Adapter Settings from Microsoft Windows: • Double-click **Network Connections** from the Windows Control Panel. • Right-click the Wireless Network Connection. • Select **Properties** from the menu. • Click **Configure** to display the Advanced settings for the adapter. **Advanced Statistics**: Select to view detailed information about the WiFi adapter and connection. See Advanced Statistics for more information. **Use Windows to manage Wi-Fi**: Select to enable Microsoft Windows XP as the wireless manager. See Microsoft Windows XP Wireless Zero Configuration for more information.

Profiles	**Manage Profiles**: Select to create or edit profiles. **Manage Exclusions**: Select to exclude networks from automatic connection. See Manage Exclusions for more information.
Help	**Intel PROSet/Wireless WiFi Help**: Starts the online help. **About**: Displays version information for the currently installed application components.

Administrator Tool (Tools menu)

The Administrator tool is for administrators or the person who has administrator privileges on this computer. This tool allows the administrator to restrict what level of control the users of this computer have over their wireless connections. This tool is used also to configure common (shared) profiles.

Users cannot modify Administrator settings or profiles unless they have the password for this tool. A password should be chosen that is secure and not easily guessed.

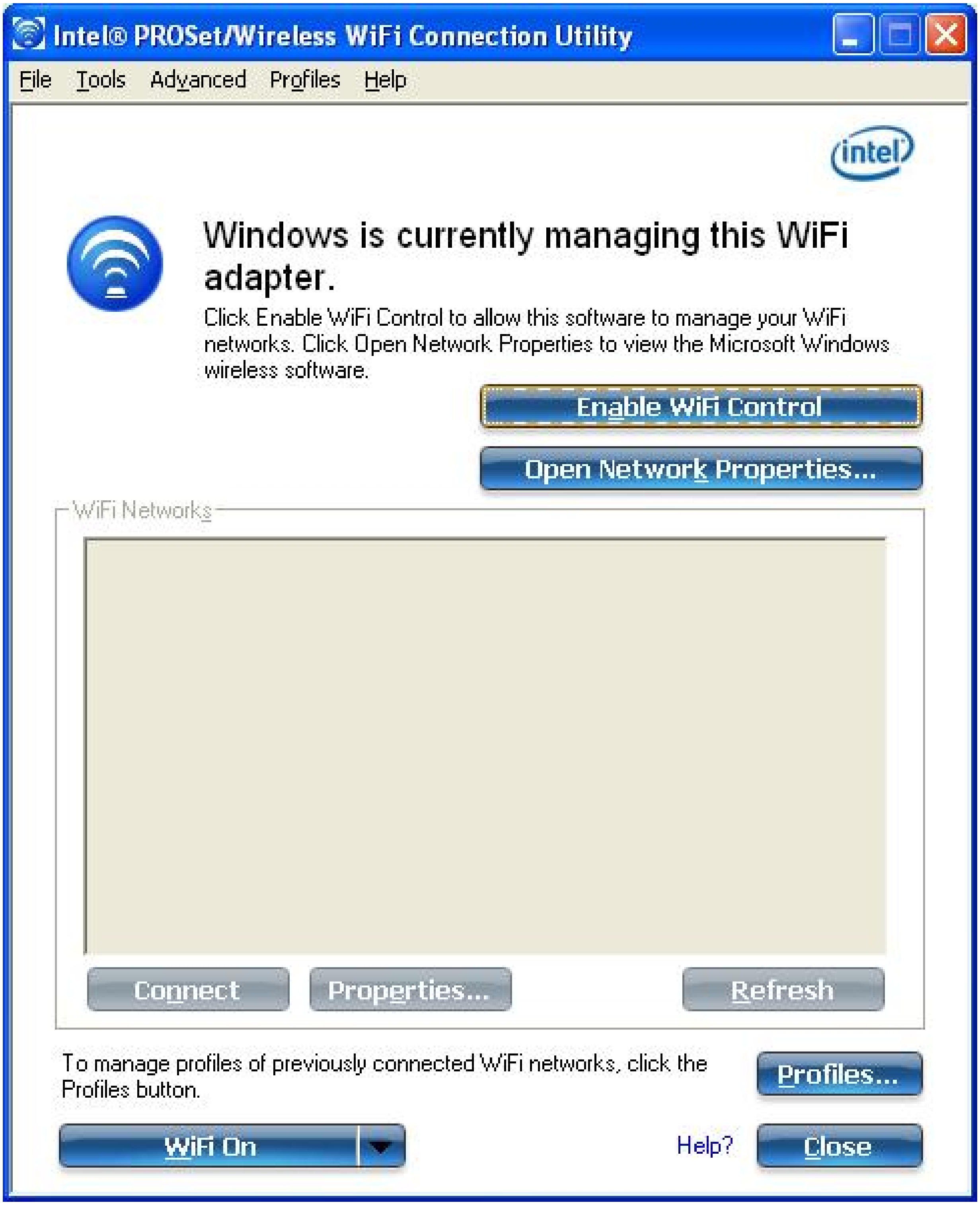
You can export these settings and profiles as one package to other computers on your network. For more information, See the Administrator Tool section.

Name	Description
Administrator Packages	The Administrator Packages are used to save administrative profiles and other settings. For Windows XP*, you can copy or send this self-extracting executable to clients on your network. When it is run, the contents are installed and configured on the destination computer. See Administrator Tool Packages.
Application Settings	An administrator can configure the WiFi connection utility Application Settings to control how the application behaves on the user's computer, and to select what level of control users have over various aspects of their wireless connections. See Administrator Tool Application Settings.
Administrator Profiles	Enable or disable Persistent or Pre-logon/Common profiles and configure Voice over IP (VoIP) settings on the computer. See Administrator Tool Profiles.
Adapter Settings	An administrator can select which level of control that users have over their wireless network connections. See Administrator Tool Adapter Settings.

EAP-FAST A-ID Groups	An administrator can select which Authority Identifier (A-ID) RADIUS server to provision Protected Access Credentials (PACs) for profiles that use EAP-FAST authentication. A-ID groups are shared by all users of the computer and allow EAP-FAST profiles to support multiple PACs from multiple A-IDs. See Administrator Tool EAP-FAST A-ID Groups.
Change Password	Change the password for the Administrator Tool. See Change Password for more information.
Close	Closes the page.
Help?	Provides help information for this page.

Use Windows to Manage WiFi (Advanced menu)

The Microsoft Windows XP Wireless Zero Configuration feature provides a built-in wireless configuration utility. This feature can be enabled and disabled within the WiFi connection utility. Click **Use Windows to manage Wi-Fi** on the **Advanced** menu. If Windows XP Wireless Zero Configuration is enabled, the features in the WiFi connection utility are disabled. To let the WiFi connection utility manage your WiFi connections, click **Enable WiFi Control** on the main window.



Installing Intel(R) PROSet/Wireless WiFi Connection Utility

Typical Installation

The following components are installed in a **Typical** installation.

- The WiFi connection utility driver. You can choose to install the driver only if desired. This is

the minimal installation.

- The WiFi connection utility. For a Typical installation, this includes the following:
  - Wi-Fi Protected Setup*
  - Intel(R) Wireless Troubleshooter

NOTE: If you plan to use Novell Client* for Windows, it should be installed prior to installation of the WiFi connection utility. If the WiFi connection utility is already installed, you should remove it prior to installation of Novell Client for Windows.

Custom Installation

The following features are available to install during a **Custom** installation. Of these, Wi-Fi Protected Setup* and Intel(R) Wireless Troubleshooter are also installed in a typical installation.

- Administrator Tool
- WMI Support
- Single Sign On
  - Pre-logon Connect
- WiFi Protected Setup
- Intel(R) Wireless Troubleshooter

Administrator Tool: Installs the Administrator Tool to the Tools menu. This tool is used to configure common (shared) profiles. The Administrator Tool is also used by an Information Technology department to enable or disable features within the WiFi connection utility.

WMI Support: Windows Management Instrumentation functionality allows administrators who do not have the WiFi connection utility installed to manage remotely clients that do have the WiFi connection utility installed.

Single Sign On: Installs the Single Sign On Pre-Login Connect feature. This tool is used to configure common (shared) profiles with the Administrator Tool. Single Sign On is targeted to the enterprise environment where users log on to their computer with a user name, password, and typically a domain. Fast User Switching does not support domain log on. The Fast User Switching and the Windows XP Welcome Screen are disabled when Single Sign On support is installed.

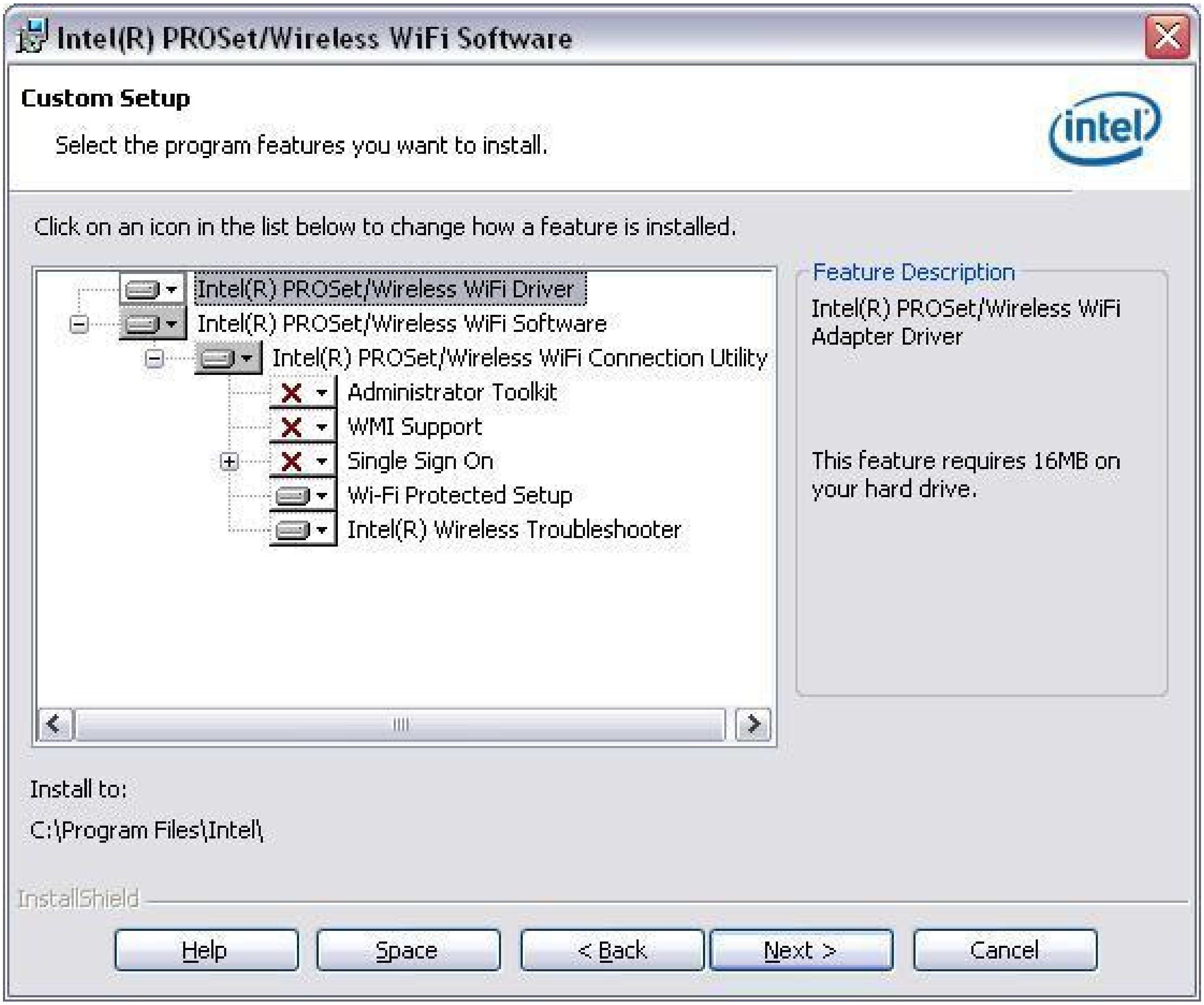
NOTE: Windows Fast User Switching is enabled by default if you use Windows XP Home Edition. It is targeted for the home user. Fast User Switching is also available on Windows XP Professional if you install it on a stand-alone or workgroup-connected computer. If a computer running Windows XP Professional is added to a domain, then Fast User Switching option is not available.

Pre-logon Connect: A Pre-logon/Common profile is active once a user logs onto the computer. Pre-logon Connect establishes a wireless connection prior to user logon to Windows. This feature is installed with Single Sign On.

WiFi Protected Setup: Installed as part of a Typical installation, this feature detects when a compatible wireless router is present and provides easy connection to it.

Intel(R) Wireless Troubleshooter: Provides valuable assistance in resolving wireless WiFi connection problems.

To install these features, select **Custom** during installation. Follow the instructions below to install features. If the WiFi connection utility is already installed, see the post-installation instructions.



Install Intel(R) PROSet/Wireless WiFi Connection Utility

1. Insert the Installation CD in your CD drive.
2. The installer presents the message:
   Welcome to the Intel(R) Wireless Installer Prerequisite Wizard. Click **Next**.
3. The next message displays:
   Welcome to the InstallShield Wizard to Intel(R) PROSet/Wireless WiFi Software. Click **Next**.
4. Read the license agreement.

5. Click **I accept the terms in the license agreement**. You can click **Print** if you want a printed copy of the agreement. Then click **Next**.
6. Click **Next** to accept the default install destination folder. Otherwise, click **Change** to specify a different location. Then click **OK** and **Next**.
7. Click **Typical** or **Custom**. If you click Typical, proceed to step 9.
8. If performing a Custom installation, select from the list of features to install. See Custom Installation for an explanation of the available features. For each feature, you can select:
   - **This feature will be installed on the local hard drive**.
   - **This feature, and all subfeatures, will be installed on the local hard drive**.
   - **The feature will not be available**.
9. Click **Next**.
10. The installation may take several minutes. When the installation completes, the message **InstallShield Wizard Completed!** displays. Click **Finish**.
11. You may be asked to reboot the computer. If so, you should reboot you computer now. Click **Yes** to do so, or **No** to reboot later.

Install Additional Software Features

If the WiFi connection utility is already installed, follow the instructions below to add the Administrator Tool and Pre-logon Connect:

1. Click **Start > Control > Panel > Add or Remove Programs > Intel PROSet/Wireless WiFi Software**.
2. Click **Change**.
3. The next message displays: **Welcome to the InstallShield Wizard to Intel(R) PROSet/Wireless WiFi Software**. Click **Next**.
4. Click **Modify**. Then click **Next**.
5. Click the red **X** next to any of the features not currently installed that you want to install.
6. For each feature you want to install, click one of the following choices, as appropriate:
   - **This feature will be installed on the local hard drive**.
   - **This feature, and all subfeatures, will be installed on the local hard drive**.
7. Click **Next**.
8. The installation may take several minutes. When the installation completes, the message **InstallShield Wizard Completed!** displays. Click **Finish**.
9. You may be asked to reboot the computer. If so, you should reboot you computer now. Click **Yes** to do so, or **No** to reboot later.

Remove Intel(R) PROSet/Wireless WiFi Connection Utility

To uninstall the WiFi connection utility:

1. Click **Start > Control Panel > Add or Remove Programs**.
2. Click **Intel PROSet/Wireless WiFi Software**.

3. Click **Change**.
4. The next message displays:
   Welcome to the InstallShield Wizard to Intel(R) PROSet/Wireless WiFi Software.
   Click **Next.**
5. Click **Remove**.
6. Click **Next.**
7. The next message appears. Make your selection from the list and click **Next**.

   Save User Defined Settings. Choose what to do with your current application:

   - **Save**. Save settings and files applicable to the current version of the application.
   - **Convert and Save**. Save settings and files in the format compatible with PROSet/Wireless WiFi version 10.
   - **Remove**. Do not save application settings.

8. The removal may take several minutes. After the software is removed, the message **InstallShield Wizard Completed!** displays. Click **Finish**.
9. A message requests that you restart your computer. Click **Yes** to restart the computer.

Back to Contents

Get Connected

Connect to a WiFi Network

You can connect to a wireless network with one of the following methods.

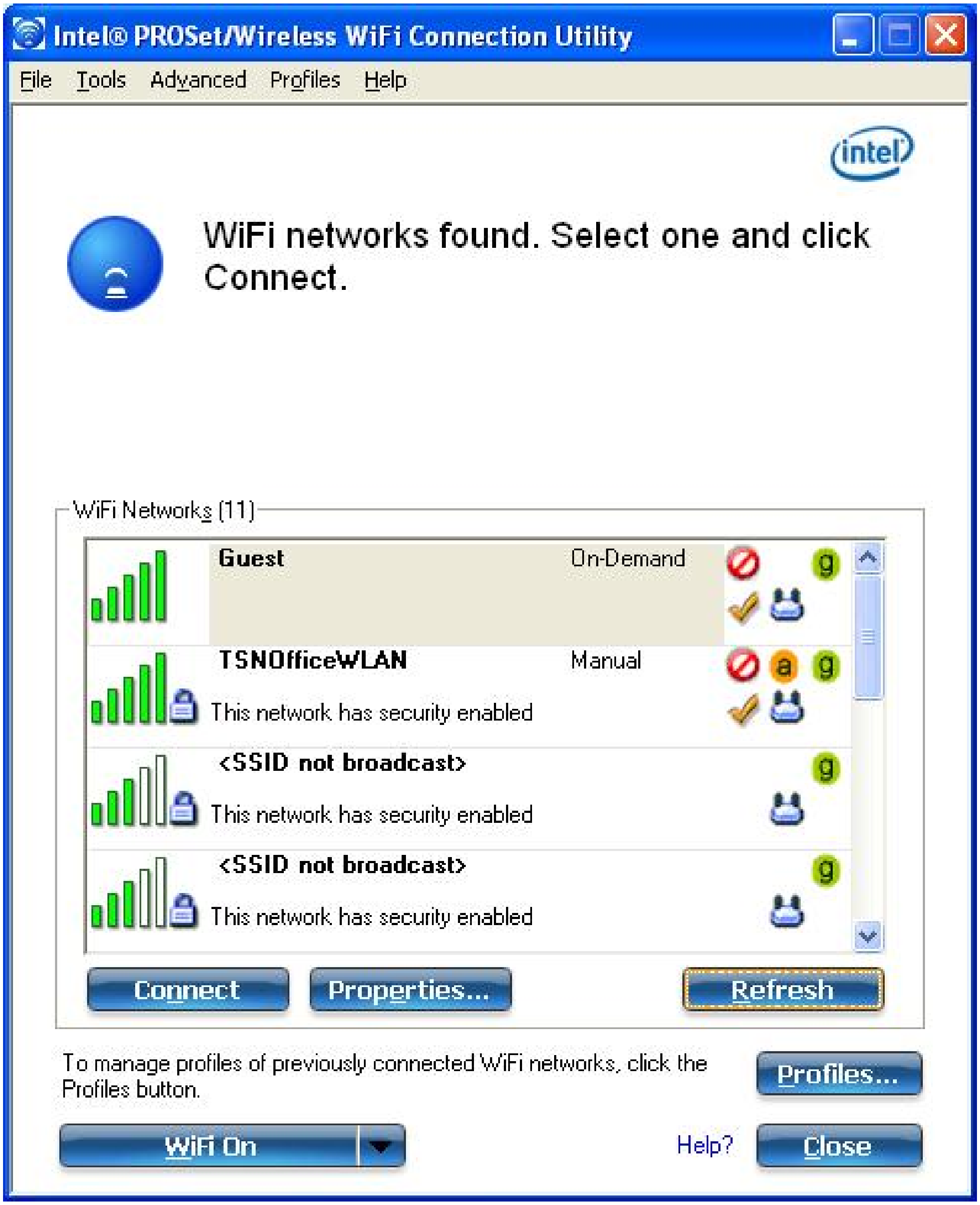
- **Automatic connection**: If an existing profile matches an available network, you are automatically connected to that wireless network.
- **Configure a new profile**: Select a wireless network from the list of WiFi networks in the Intel(R) PROSet/Wireless WiFi Connection Utility main window. Click **Connect**. If you successfully connect, a profile is created in the Profiles list for future use.
- **Connect to a profile in the Profiles list**: You can select a profile from the Profiles list. To activate it, click **Connect**. This lets you connect to a network that is lower in the list (if it is available).
- Right-click the Taskbar icon located in the lower right corner of your Windows desktop. Click **Connect to Profile**. A list of previously configured profiles is listed. Select a profile.

First Time Connection

The WiFi connection utility automatically detects WiFi networks that are within range of your WiFi adapter. When a network is found, a desktop alert notification displays: **WiFi networks found**. See Taskbar Icons for more information.



1. Double-click the desktop alert to open the WiFi connection utility main window.
2. Select a network from the WiFi Networks list.



3. Click **Connect**. If the network does not require security authentication, a desktop alert notifies you that you are connected to the network. See Main Window and Taskbar for more information about the taskbar menu and icons.
4. If the network has security enabled, the Profile Wizard opens the Configure WiFi Settings window. This guides you through the process of creating a WiFi profile for this network. After a profile is created, connecting to this network in the future will be much easier.
5. You are requested to specify a **Profile Name**. The **Profile Name** is your name for this network. You can accept the existing profile name if present, or enter one. The profile name can be anything that helps you identify this network. For example, My Home Network, Coffee Shop on A Street.
6. You are requested to specify **WiFi Network Name (SSID)**: This contains the network identifier name. This is a unique identifier that differentiates one WiFi network from another. If one is already entered, you can keep that.
7. Click **Next**. The Profile Wizard then detects the security settings of this network. The information you enter depends on those security settings. For information about security settings, see Security Settings. For more information about keys and passwords, see Network Keys. For more information about profiles, see Profiles. You may need to contact the network administrator for the information

needed to log into this network.
8. After entering the required information, click **OK** to connect to the wireless network.

See Main Window for more information.

Using Wi-Fi Protected Setup* to Configure or Join a Network

- Configure an access point and set up a network
- Connect an enrollee (computer) to a network or access point
- Add an enrollee to a network at the registrar

Intel(R) PROSet/Wireless WiFi implements Wi-Fi Protected Setup* to permit easy and secure set up and management of a wireless network. You can use this capability to initially set up a wireless network and to introduce new devices to the network. Wi-Fi Protected Setup simplifies the set up process and at same time helps ensure that the network is configured securely. The following terms are used in this discussion.

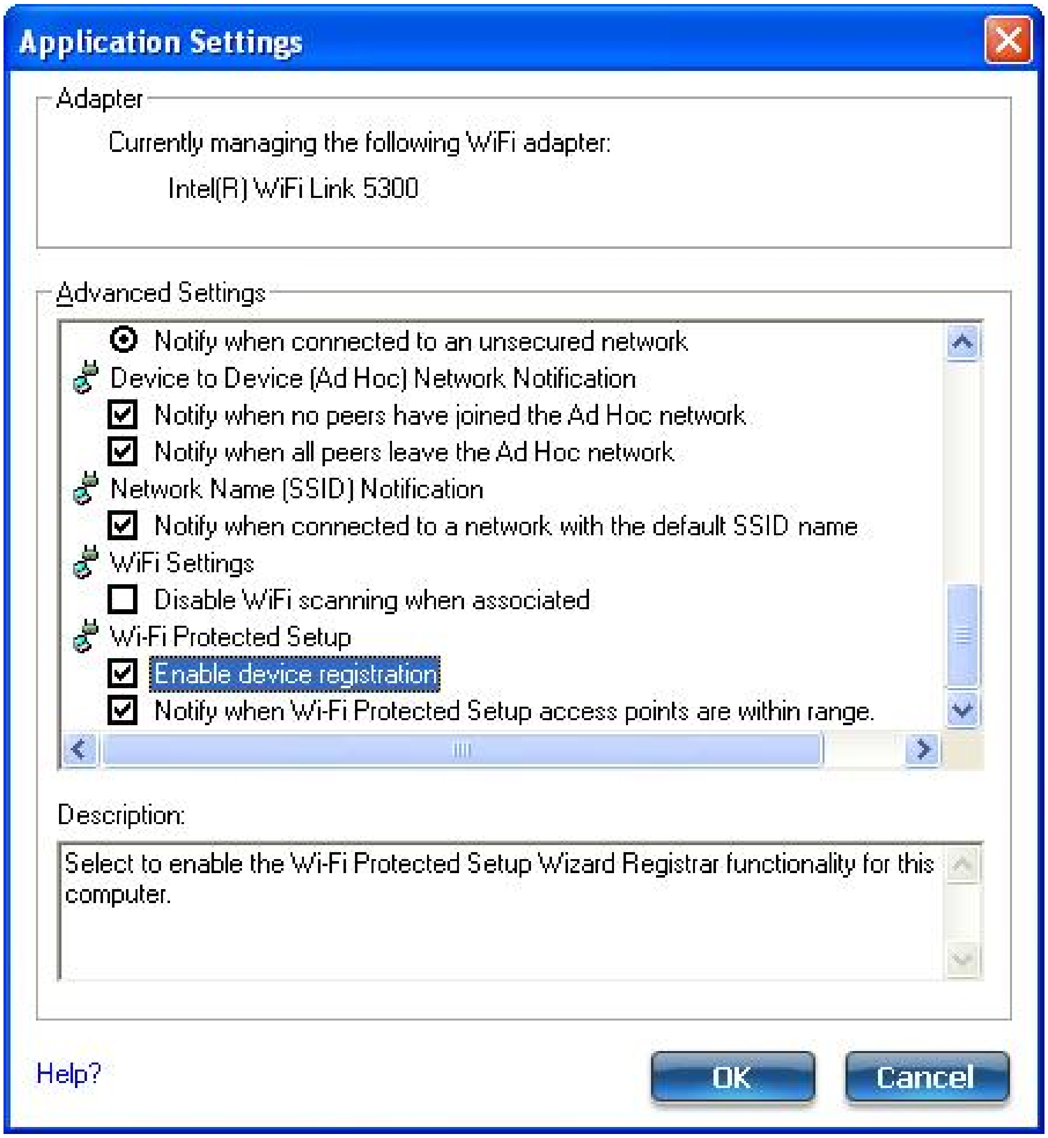
- **Access Point**: A device that connects wireless devices to a network. The access point is configured with the necessary network name (SSID) and security credentials.
- **Enrollee**: A device that seeks to join an access point or wireless network, but does not have the password or key for the access point or network. Once the computer obtains the valid password or key, it becomes a member of the wireless network. The WiFi connection utility can be configured to operate as an enrollee for a supported access point.
- **Registrar**: A registrar is a logical entity (usually a computer) that allows other devices (usually computers) to join the wireless network. The WiFi connection utility can be configured to operate as a registrar for a supported access point(s). The registrar securely transfers the access point key or password automatically.

A new wireless network is established by configuring the access point, connecting the desired computers equipped with WiFi adapters, and optionally attaching external network connectivity (i.e. the Internet, typically by connecting the access point to a DSL or cable modem, or equivalent).

Configure an Access Point and Set up a Network

The following steps will configure this computer as a registrar for a secure network or access point.

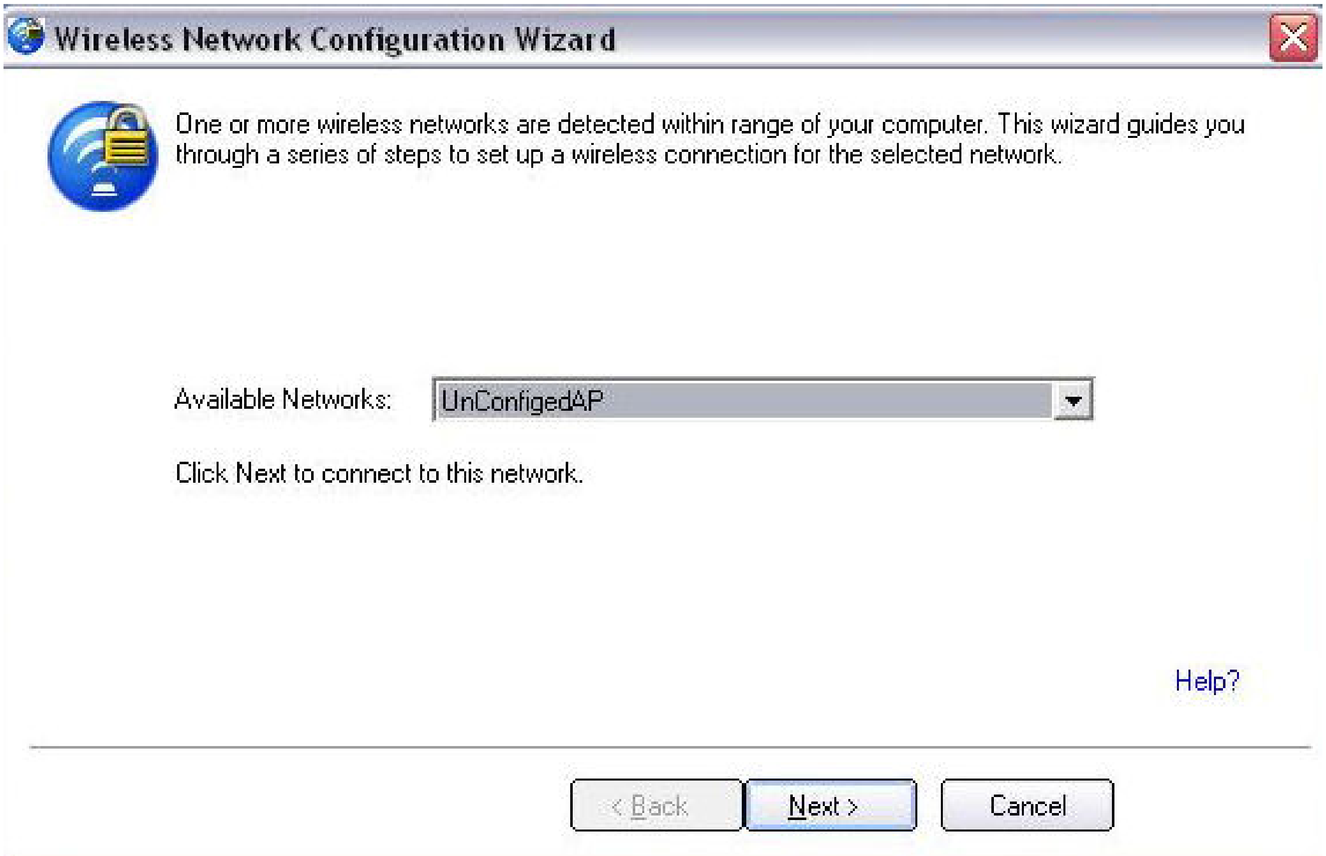
1. Locate the device ownership password for the access point. This is set by the manufacturer of the access point. The password is often located on a label on the bottom of the device.
2. Turn on the network access point.
3. At the computer that you want to establish as the registrar, turn on the WiFi connection utility.
4. In the WiFi connection utility, click **Tools** > **Application Settings**.
5. In the Advanced Settings area under Wi-Fi Protected Setup, turn on **Enable device registration**.



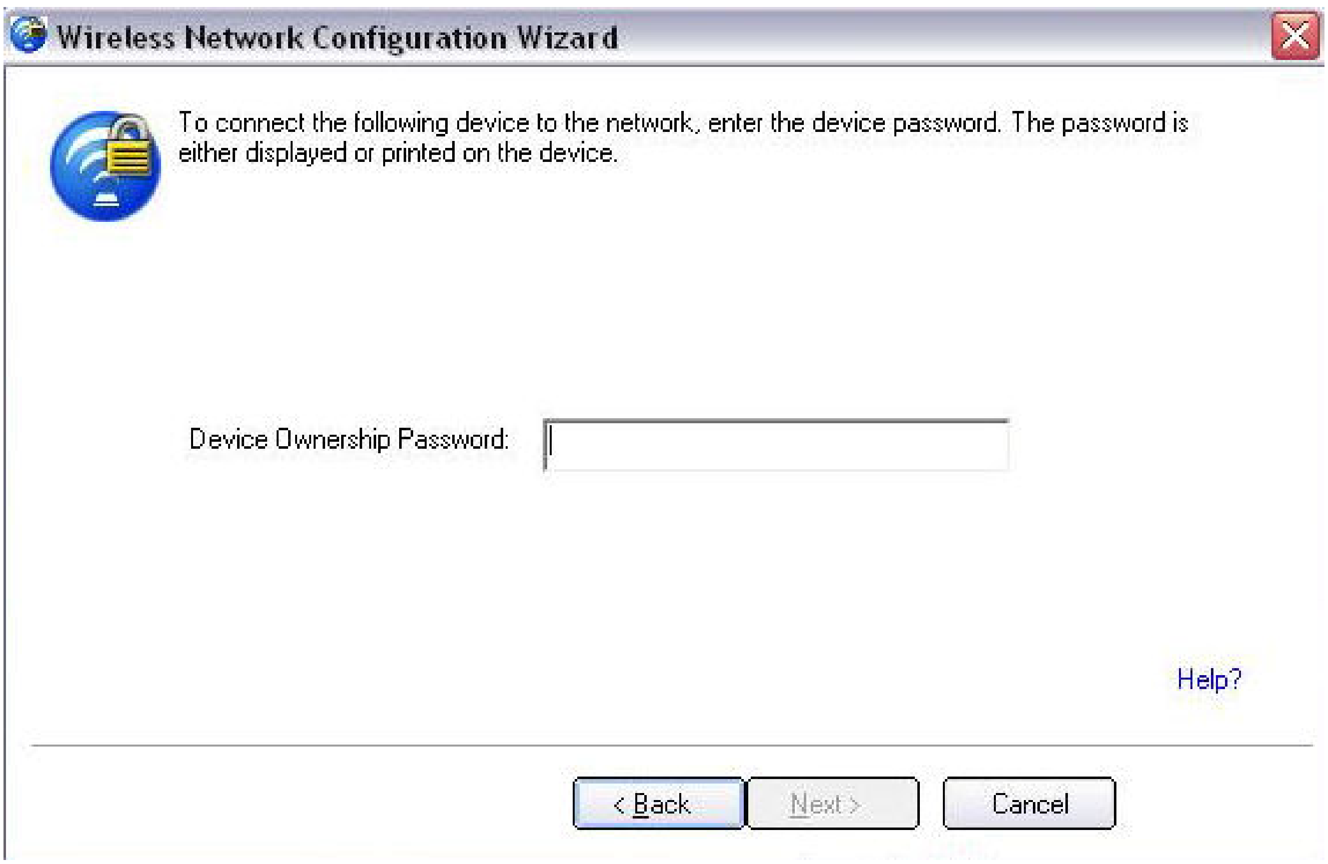
6. The next message tells you that one or more compatible devices are within range of your computer. Click this message. (Or, you can select the network from the WiFi Networks list in the WiFi connection utility main window.)



7. At the next window, on the Available Networks list, select the network that you want to connect to. The listed network depends on what is detected. Click **Next**.



8. At the next window, enter the Device Ownership Password that you retrieved from the access point in step 1. Click **Next** to continue.

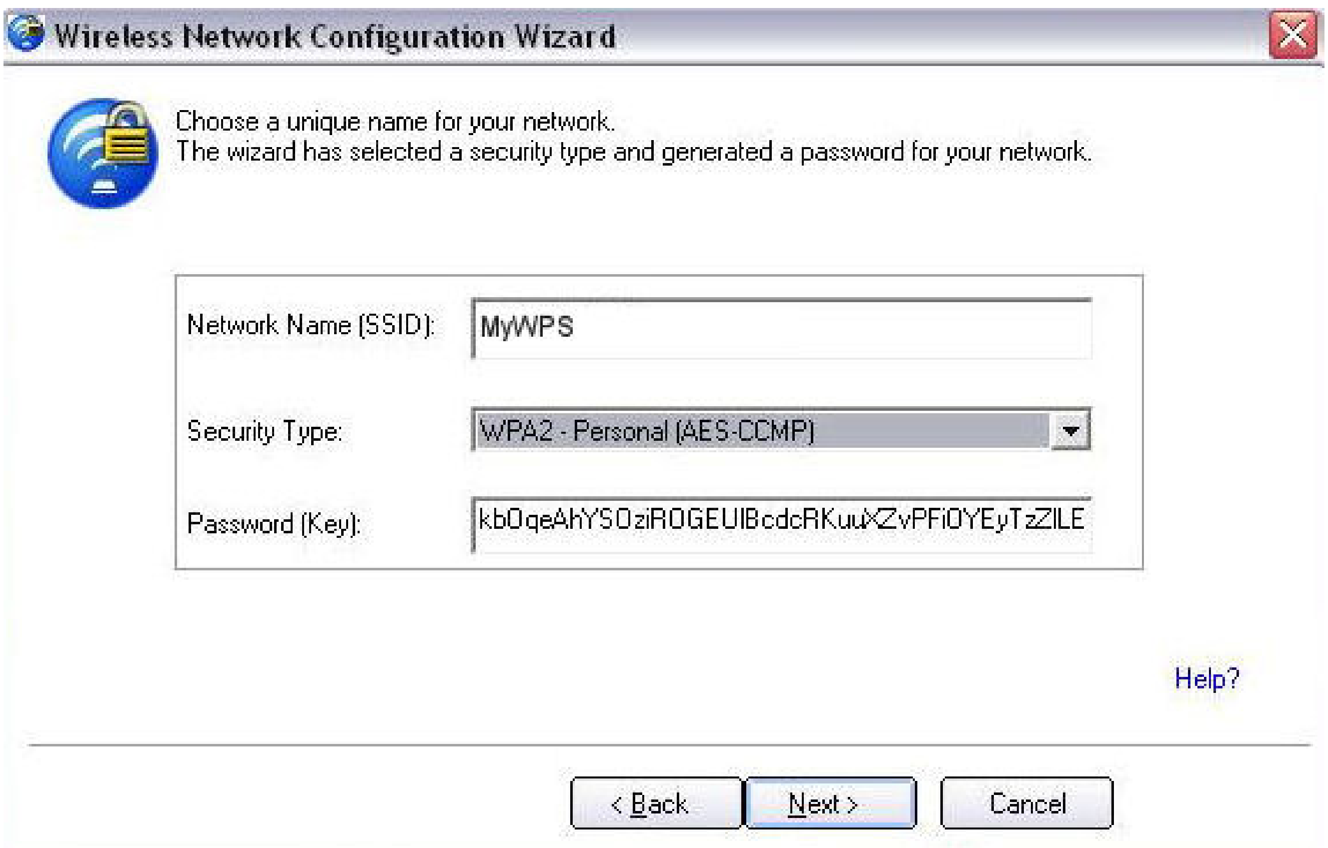


9. The next window shown displays the **Network Name**, **Security Type**, and **Password**. If the access point is *already configured*, it is grayed out; proceed to step 10. If the access point is *not configured* (fields are *not* grayed out), proceed to step 11.
10. After a few seconds the following message is displayed:

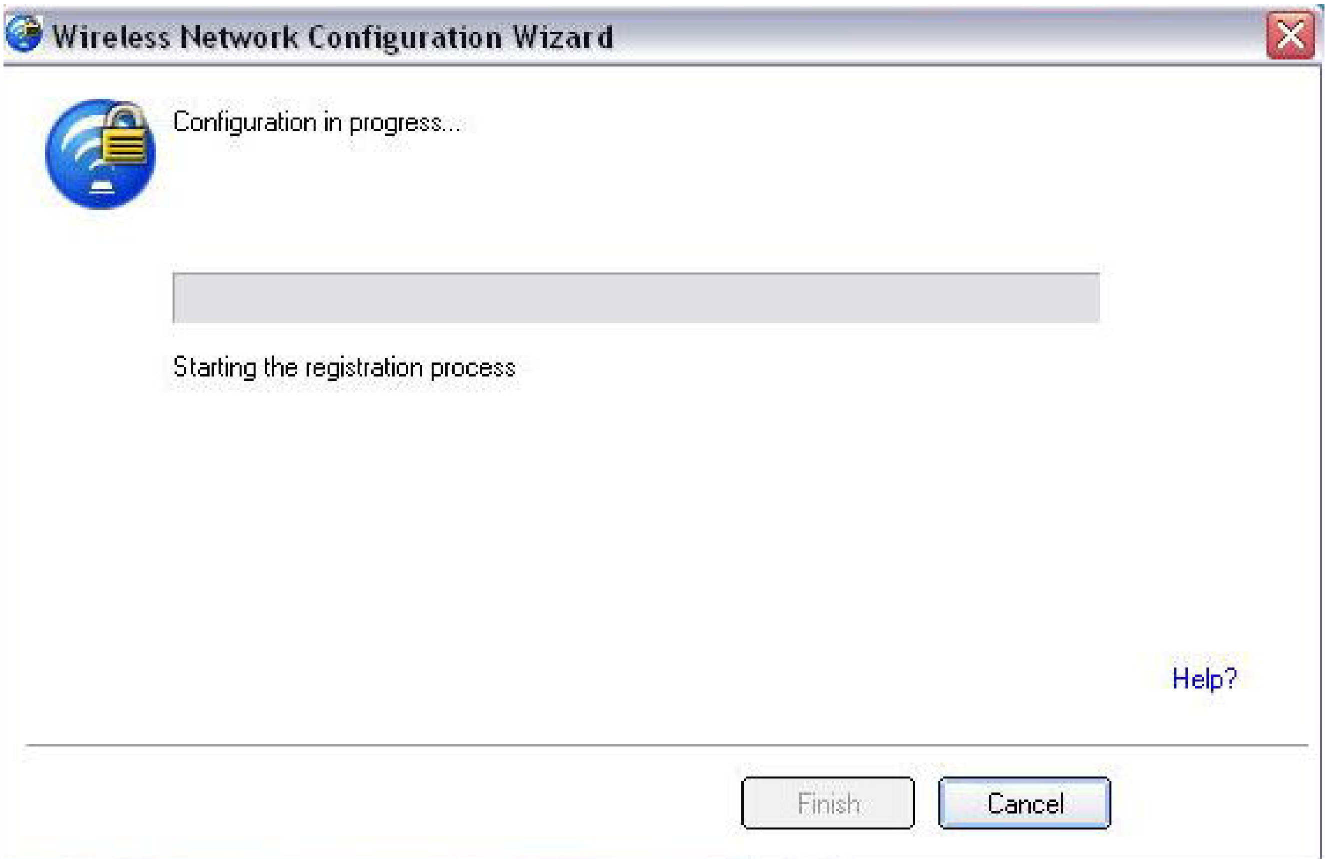
The access point is already configured. Do you want to reconfigure it?

If you do not want to reconfigure the access point, select **No**. The software joins the network, makes the connection, and creates a profile. It then exits and this procedure is completed. If you want to reconfigure the access point, select **Yes**.

11. The next window is displayed. The first field shows the name of the access point. This is by default the **Network Name (SSID)**. In this example we have reset it to MyWPS. You can name it whatever you want.
12. In the **Security Type** field, select the security type you want.
    - WPA* Personal requires manual configuration of a pre-shared key (PSK) on the access point and clients. This PSK authenticates a password or identifying code, on both the client station and the access point. An authentication server is not needed.
    - WPA2* is the second generation of WPA security that provides enterprise and consumer wireless users with a high level of assurance that only authorized users can access their WiFi networks. Here we have selected WPA2 Personal security. You can use Intel PROSet/Wireless WiFi profiles to obtain the WiFi network name (SSID) and WPA2-Personal pass phrase to use for a legacy device.
13. The third field is the **Password (Key)**. The password shown is randomly generated or pre-configured, you can change it to whatever password you want. However you should use a robust key for improved security. It must have between 8 and 63 characters. When you have completed this step, click **Next**.



The following windows show the configuration of the access point and the registrar.

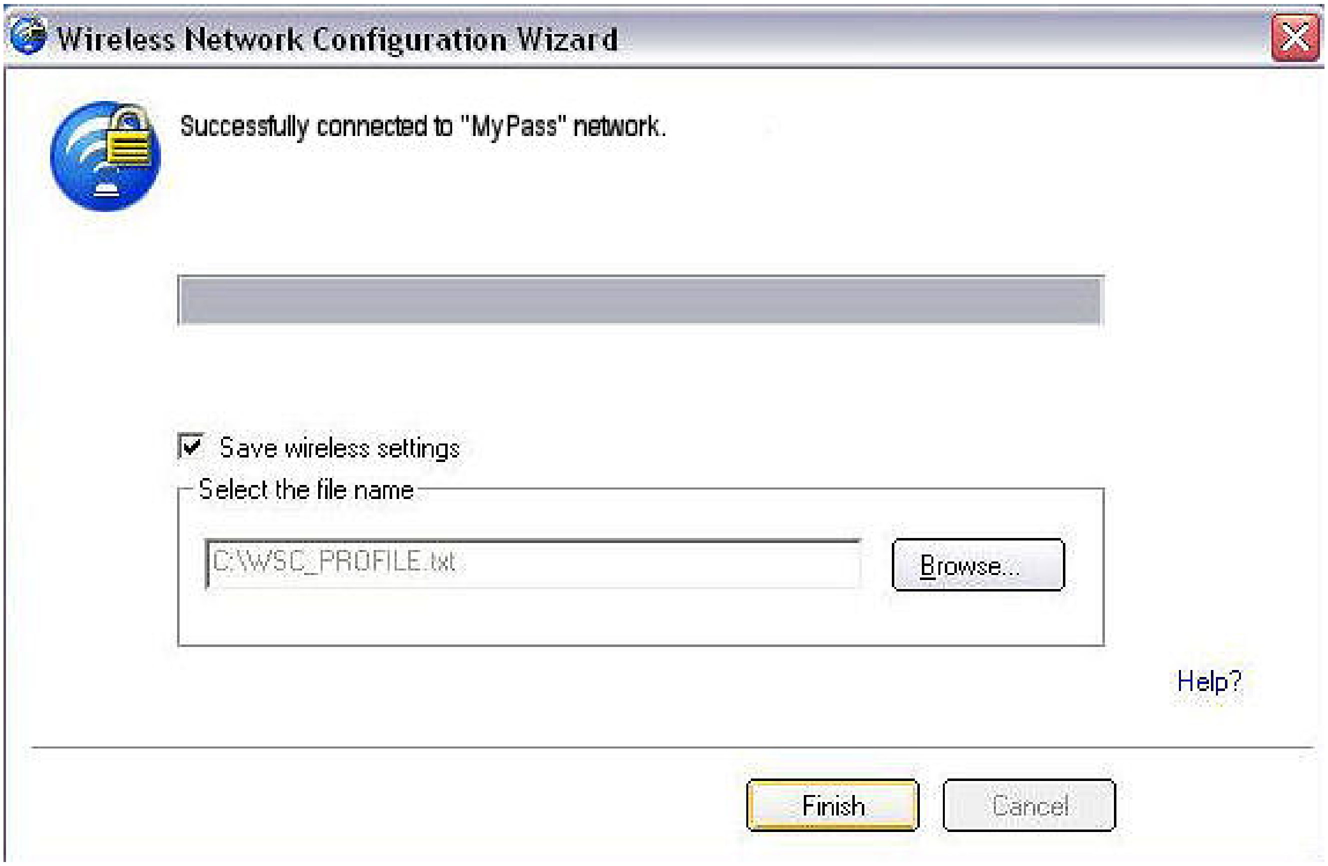


The following window appears briefly and shows the configuration of wireless settings for the access point.



14. After the network receives the Ownership Password, you are notified that you have **Successfully connected to <name of wireless network>**. Click **Finish**. This process completes configuration of

the access point and the registrar.



15. If you want to save these settings to a profile for future use by a legacy client, click **Save wireless settings**. The profile settings are saved to a text file (txt) on your local hard drive. The file is saved to your local C:\ drive by default. Accept the default save location or click **Browse** to choose another location on your computer.

Next, you can connect an enrollee (computer) to the network using the registrar.

Connect an Enrollee to a Network or Access Point

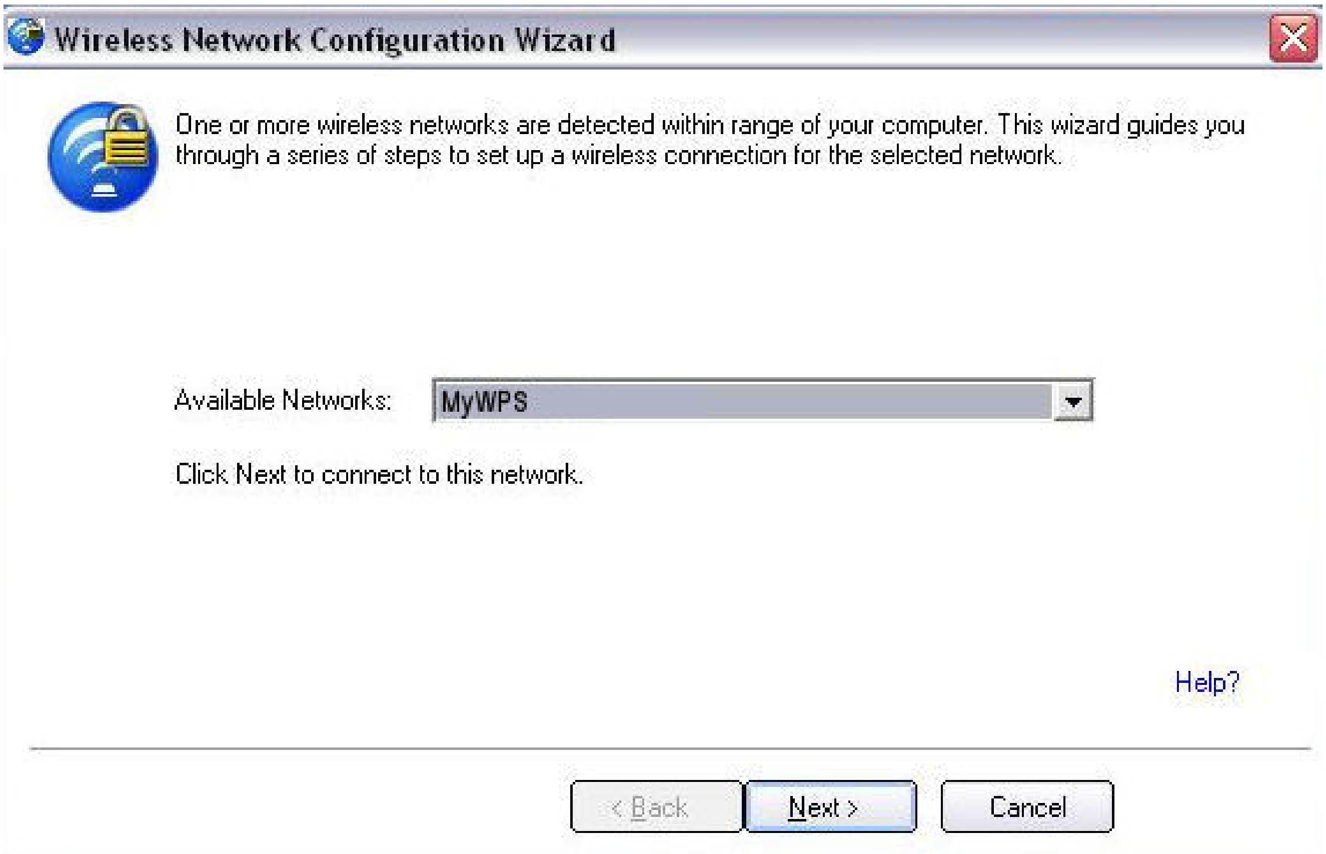
Perform these steps to connect an enrollee to the network you just created. This assumes that the registrar computer is running the WiFi connection utility.

NOTE: To achieve transfer rates greater than 54 Mbps on 802.11n connections, WPA2-AES security must be selected. No security (**None**) can be selected to enable network setup and troubleshooting.

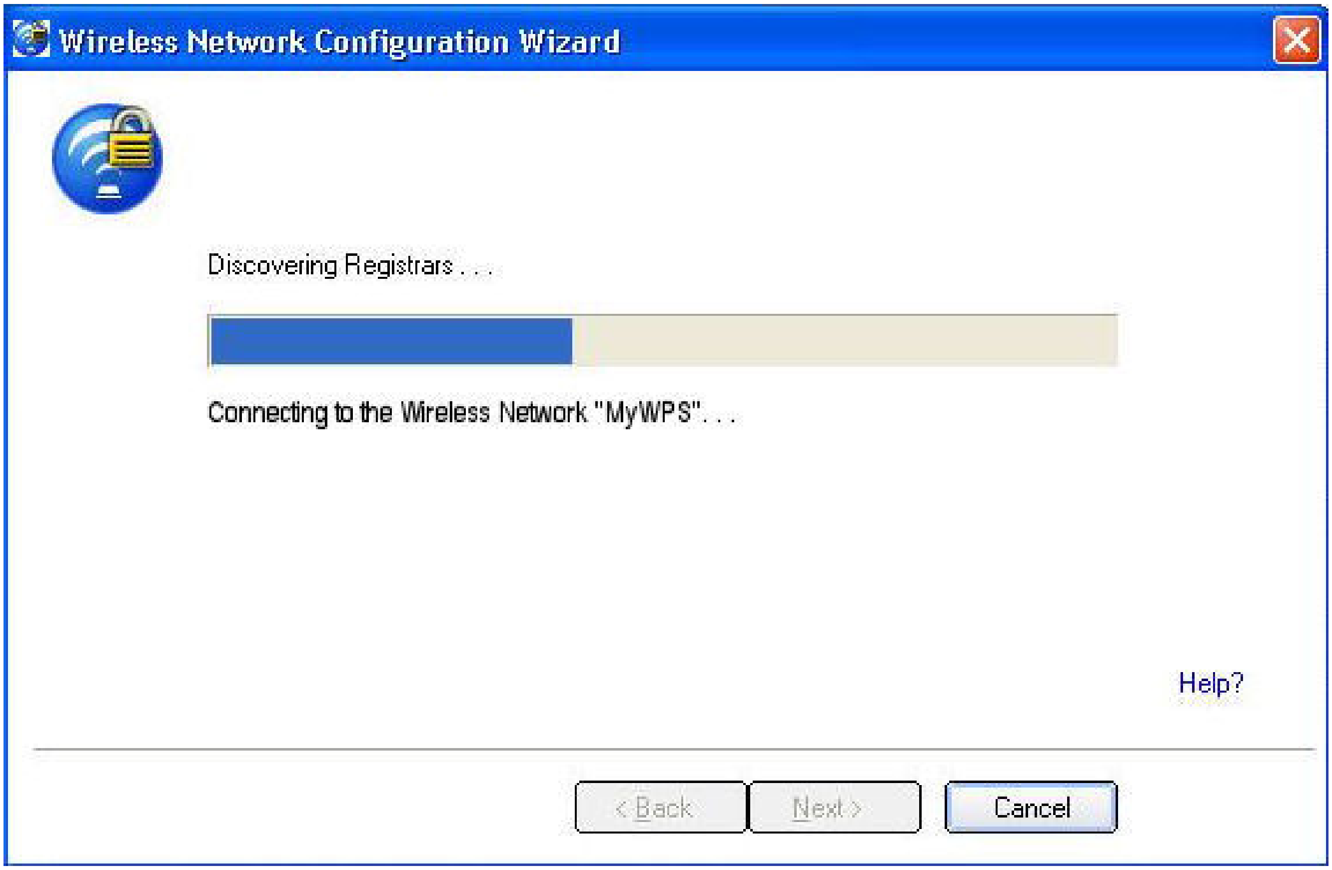
1. At the enrollee you want to connect the network, a message tells you that one or more access points with Wi-Fi Protected Setup capability is within range of your wireless computer. Click on this message. (Or, you can select the network from the WiFi Networks list in the WiFi connection utility main window.)



2. The **WiFi Network Configuration** start up page opens. Use the Available Networks list to select the network that you want to connect to (in this example it is MyWPS). Then click **Next**.



3. The Discovery window opens. The enrollee that you want to connect to the network discovers the registrar for the network. Assuming that the Discovery process succeeds, the name of the registrar or access point is displayed.

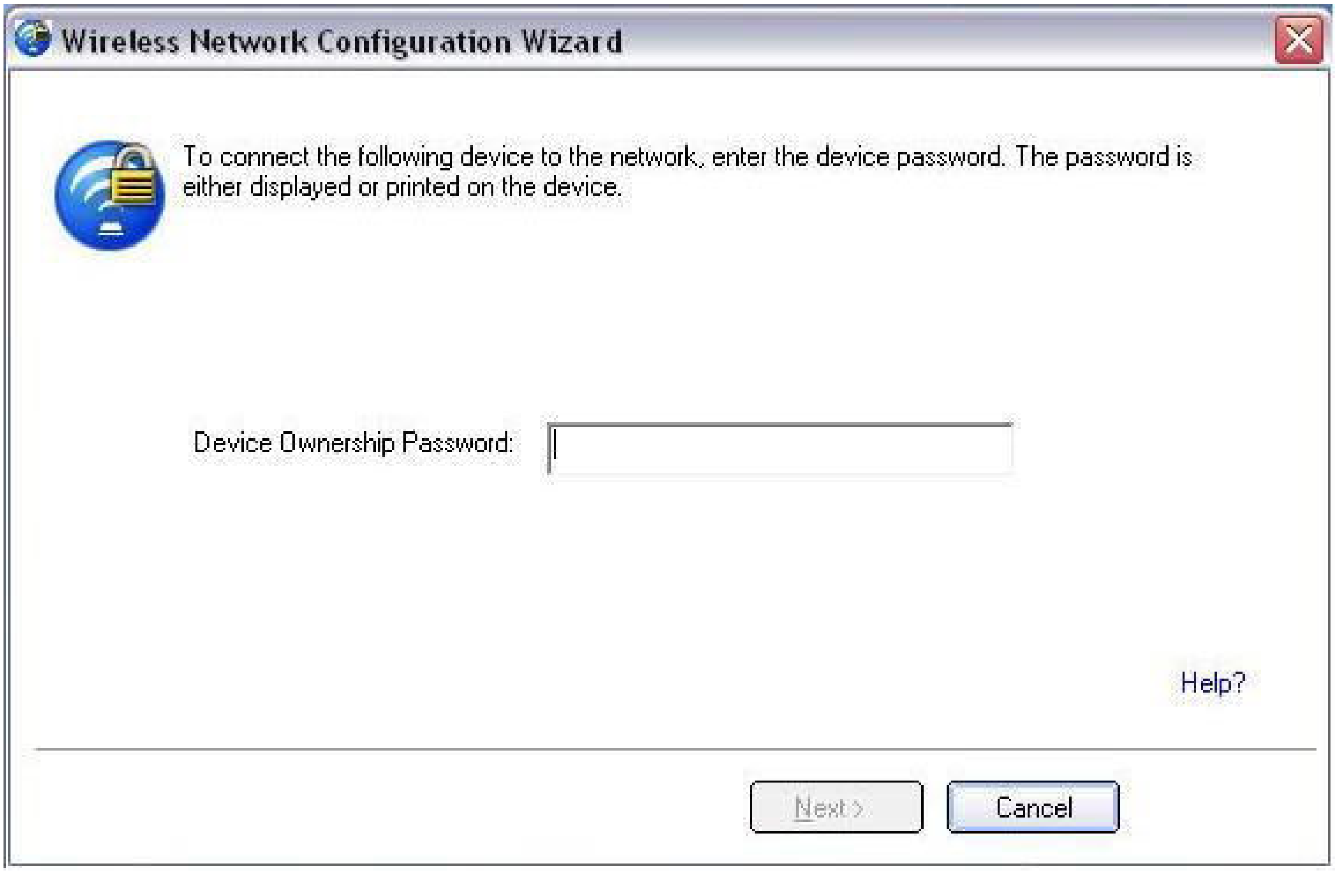


4. The next window appears, displaying the Device Password (enrollee password). The password displayed at the enrollee is a unique, randomly generated temporary password for the enrollee. This password is used to ask permission to connect to the network access point. (The password shown below is an example only.).



5. At the registrar, enter the password provided by the enrollee. Then click **Next**.

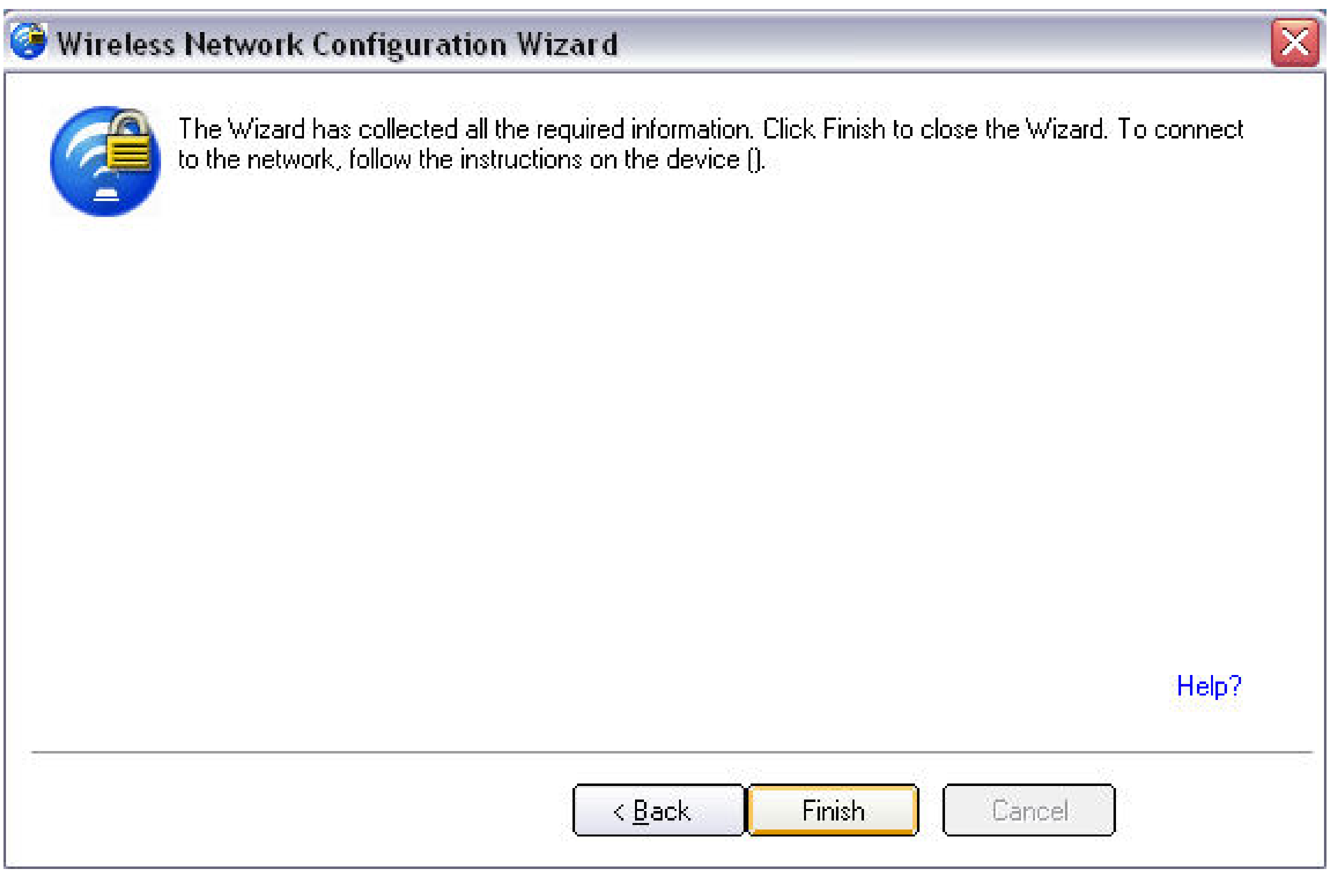
NOTE: This process assumes that the registrar is running the WiFi connection utility; the process and windows displayed at the registrar may be different for software from other vendors. Some access points may have a built in registrar.



6. The next window lists the profile for this network. The selected profile will be sent to the enrollee, granting it access to the network. Only supported profiles are displayed. Supported profiles are those based on WPA-PSK, WPA2-PSK, and Open (None) security. Select the profile and click **Next** to finalize the enrollment process.



7. The last window shows that the enrollee registration with the registrar is complete. Click **Finish**.



8. At the enrollee, click Next. At the enrollee, you are notified when you have **Successfully connected to <name of wireless network>**. Click **Finish**.

Add an Enrollee to an Existing Network at the Registrar

This following procedure lets you add an enrollee to an existing network, where the access point is already configured and the registrar has already joined the AP.

NOTE: This process assumes that the registrar is running the WiFi connection utility; the process and windows displayed at the registrar may be different for software from other vendors.

1. Get the Device Password for the enrollee computer that you want to add to the network.
2. At the task tray icon for the WiFi connection utility, right-click and select **Add New Device**.
3. Perform steps **5** through **8** of the procedure Connect an Enrollee to a Network or Access Point.

Other Wireless Managers

If the WiFi connection utility detects another software application trying to communicate with the wireless device, you are notified of this behavior.

Microsoft Windows XP* Wireless Zero Configuration

To switch from the Intel(R) PROSet/Wireless WiFi Connection Utility to the Microsoft Windows XP Wireless Zero Configuration, perform these steps:

1. At the Intel(R) PROSet/Wireless WiFi Connection Utility main window, under the Advanced menu, select **Use Windows to manage WiFi**.
2. At the prompt window, you are queried: Do you want Windows to manage your WiFi network connections? Click **Yes**.
3. Click **Close** to close the Intel(R) PROSet/Wireless WiFi Connection Utility.
4. Right-click on the tasktray icon and select **Open Wireless Zero Configuration**.

   NOTE: Any wireless profiles created in the WiFi connection utility are not visible in Microsoft Windows XP Wireless Zero Configuration. If you want to use your Intel wireless profiles, click **Enable Intel PROSet/Wireless WiFi** on the main window.

When you are finished using the Microsoft Windows XP Wireless Zero Configuration, you can switch back to the WiFi connection utility To do this, click **Enable Intel PROSet/Wireless WiFi** on the WiFi connection utility main window.

Third-Party Wireless Software

If you use software provided by a hotspot location (coffee shop, airport terminal), the WiFi connection utility notifies you and then disables itself. It cannot manage the wireless device when another wireless manager communicates with the wireless device. To take advantage of the WiFi connection utility features, you want to disable or remove this software when you leave the hotspot.

Back to Top

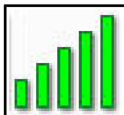
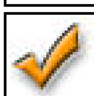
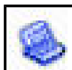
Back to Contents

Trademarks and Disclaimers

Back to Contents

WiFi Networks list

The WiFi Networks list displays a list of WiFi networks within range of the adapter. To update the list, click **Refresh** to rescan for WiFi networks. Click **Profile** to launch the Profile Wizard and create a profile for the selected wireless network.

Name	Description
WiFi Networks ( )	The number within the parentheses designates the number of wireless network found within range of your wireless network adapter.
	The signal strength of the wireless network access point or computer (Device to Device [ad hoc] mode). The signal strength icon bars indicate that the wireless network or computer is available for connection but is still not associated with an access point or computer (Device to Device [ad hoc] mode).
Network Name	**Network Name (SSID)**: The name of the network that the adapter is connected to. The Network Name (SSID) must be the same as the SSID of the access point. If an access point does not broadcast its network name (SSID) or the WiFi adapter receives a hidden network name from a stealth access point, **<SSID not broadcast>** is displayed in the WiFi Networks list. To associate with an <SSID not broadcast> network entry, a new profile must be created before connection. After connection, the <SSID not broadcast> is still displayed in the WiFi Networks list. The associated SSID profile is viewed in the Profiles list.
Status	Notification that the adapter is connecting to the wireless network. Once connected, the status is changed to **Connected**.
	**Profiles**: Identifies a network in the WiFi Networks list that is connected and has a profile in the profiles list.
	The wireless network uses Network (Infrastructure) mode.
	The wireless network uses Device to Device (ad hoc) mode.
	The wireless network uses Security encryption.

	The band frequency being used by the wireless network (802.11a, 802.11b, 802.11g, or 802.11n).
	The wireless network is on the Exclude list or the profile is configured for **Manual** connection. When set to Manual in the profile, connection to network or an access point is not automatic. Double-click on the network in the list to connect to it.
Connect (Disconnect)	Click to connect to a wireless network. Once connected, the button changes to **Disconnect**. Lists the network names of the available networks and profiles. The network status icons indicate the current connection status. • If the selected network has 802.1X authentication, the Profile Wizard General Settings opens. If the network has no WEP security (Open), WEP 64-bit or 128-bit encryption, or pre-shared key (PSK), click **Connect**. • If a PSK or WEP password are required, you are prompted to enter this information prior to connection. If you need to add security settings, click **Advanced** to access the **Create WiFi Profile General Settings**. See First Time Connection for more information.
Properties	Provides detailed information about the connected network and its access points. See Network Properties for information.
Refresh	Refreshes the list of available networks. If any new networks are available within range of the adapter, the list is updated to show the new network name.
WiFi On / WiFi Off	Switch the WiFi radio off and on. See Turn WiFi On or Off for more information.
Close	Closes the Intel(R) PROSet/Wireless WiFi Connection Utility main window.
Help?	Provides help information for this page.

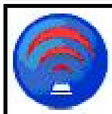
Back to Top

Back to Contents

[Back to Contents](#)

Connection Status Icons

The connection status icons indicate the current connection status of your WiFi adapter. The connection status icon displays in the Intel(R) PROSet/Wireless WiFi Connection Utility main window. The Taskbar icon also indicates the current connection status. See Taskbar Icons for more information.

Icon	Description
	**WiFi turned off**: The WiFi adapter radio is turned off. Click the **WiFi On** button to turn on the radio.
	Indicates connection problems including authentication failures.
	**Searching for WiFi networks**: The WiFi adapter is scanning for any available WiFi networks. **Animated Icons**: 
	**No WiFi networks found**: The adapter does not find any available WiFi networks.
	**Wireless network found**: An available wireless network is found. You can choose to connect to available networks displayed in the WiFi Networks list.
	**Connecting to a wireless network**: You are connecting to a wireless network. The crescent shaped curves switch between green and white until an IP Address is obtained or if a connection error occurs.
	**Connected to a wireless network**: You are connected to a wireless network. The network name, speed, signal quality, and IP address display the current connection status. Click the Details button to display details of the current network connection.
Network Name	**Name (Profile Name or SSID)**: The name of the network that the adapter is connected to. The Name column displays the SSID or the Profile name if a profile for the network is available.
Signal Quality 	The signal strength icon bars indicate the quality of the transmit and receive signals between your WiFi adapter and the access point or computer in Device to Device (ad hoc) mode. The number of vertical green bars indicates the strength of the transmit and receive signals. **NOTE**: The signal strength is displayed for the closest AP for networks that contains multiple APs. The signal strength ranges from excellent to out of range. The following factors affect signal strength: • Signal quality decreases with distance and is affected by metal and concrete barriers. • Metal objects can reflect signals and cause interference. • Other electrical devices can cause interference.

Properties	Provides adapter connection status information. See Network Properties for information.
WiFi On / WiFi Off	Switch the radio off and on. See Turn Radio On or Off for more information.
Help?	Provides help information for this page.
Close	Closes the WiFi connection utility main window.

Back to Top

Back to Contents

Back to Contents

Network Properties

Click Properties at the Intel(R) PROSet/Wireless WiFi Connection Utility main window to see detailed information about the selected network and its access points. This screen shows you information about this network, information about the access points, and also lets you open up the Exclude List Management screen. On the Exclude List Management screen, you can add profiles to be excluded from automatic connection.

Network Properties details

Name	Description
Network Name	Displays the WiFi network name.
Band	Current band and frequency being used. Displays **Out of Range** if no band and frequency are displayed. The following bands are listed: • 802.11a • 802.11b • 802.11g • 802.11n

Operation Mode	Displays the current mode: • Network (Infrastructure) A wireless network centered around an access point. In this environment, the access point not only provides communication with the wired network, but also mediates wireless network traffic in the immediate neighborhood. • Device to Device (ad hoc) A communication configuration in which every computer has the same capabilities, and any computer can initiate a communication session. Also known as a peer-to-peer network or a computer-to-computer network.
Authentication Level	Displays the current authentication security mode for the network being used. The following network authentication levels are listed: • Open • Shared • WPA-Enterprise • WPA2-Enterprise • WPA-Personal • WPA2-Personal Displays the authentication used by the currently used network. See to Security Overview for more information.
Data Encryption	The following Data Encryption settings are listed: • None • WEP • TKIP • CKIP • AES-CCMP See to Security Overview for more information.

Access Points in this Network <0-50>	• **Signal Strength**: The signal strength icon bars indicate the strength of the transmit and receive signals between your WiFi adapter and the nearest access point. • Displays one of the following icons:  . Indicates the band being used **(802.11a, 802.11b, 802.11g or 802.11n)**. • **Channel**: Displays the current transmit and receive channel being used for a particular wireless network. • **BSSID (Infrastructure operating mode)**: Displays the twelve-digit MAC address of the access point of the selected network.
Manage Exclusions	See Manage Exclusions for more information. If network exclusion is enabled (see Application Settings), then the Network Properties also indicates if the network is excluded from automatic connection.
Close	Closes the Network Properties.
Help?	Provides help information for this page.

Back to Top

Back to Contents

Back to Contents

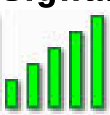
Network Connection Details

When you are connected to a network, click the **Details** button on the Intel(R) PROSet/ Wireless WiFi Connection Utility main window to display the Connection Details.



Connection Details Description

Name	Description
Profile Name	Name of the profile.
Network Name	Network Name (SSID) of the current connection.

Signal Quality	A radio frequency (RF) signal can be assessed by two components: • signal strength (quantity) • signal quality The quality of the signal is determined by a combination of factors. Primarily it is composed of signal strength and the ratio of the RF noise present. RF noise occurs both naturally and artificially by electrical equipment. If the amount of the RF noise is high, or the signal strength is low, it results in a lower signal to noise ratio, which causes poorer signal quality. With a low signal to noise ratio, it is difficult for the radio receiver to discern the data information contained in the signal from the noise itself.
Signal Strength 	The signal strength icon bars indicate the quality of the transmit and receive signals between your WiFi adapter and the access point or computer in Device to Device (ad hoc) mode. The number of vertical green bars indicates the strength of the transmit and receive signals. **NOTE**: The signal strength is displayed for the closest AP for networks that contains multiple APs. The signal strength ranges from excellent to out of range. The following factors affect signal strength: • Signal quality decreases with distance and is affected by metal and concrete barriers. • Metal objects can reflect signals and cause interference. • Other electrical devices can cause interference.
IP Address	**IPv4 Address**: Internet Protocol (IP) address for the current connection.
	IPv6 Address: The next generation IP address is backward compatible and is designed to fix data security problems with IPv4. IPv6 increases the address space from 32 to 128 bits, providing for an unlimited number of networks and systems. It also supports quality of service (QoS) parameters for real-time audio and video.

Adapter MAC Address	Media Access Control (MAC) address for the WiFi adapter.
Band	Indicates the wireless band of the current connection. • 802.11a • 802.11b • 802.11g • 802.11n
Number of Antennas in Use	This indicates the number of antennas currently in use. This number depends on the band(s) that the various networks are currently using, the transmit/ receive modes in use on those bands, the signal strength, and the capabilities of the access point(s). The user has no direct control over this parameter.
Supported Data Rates	Rates at which the WiFi adapter can send and receive data. Displays the speed in Mbps for the frequency being used. • 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 • 802.11b: 1, 2, 5.5, and 11 • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 • 802.11n: 300, 270, 243, 240, 180, 150, 144, 135, 130, 120, 117, 115.5, 90, 86.667, 72.2, 65, 60, 57.8, 45, 43.3, 30, 28.9, 21.7, 15, 14.4, 7.2
Radio Frequency	Displays the frequency of the current wireless connection. • 802.11a: 5.15 GHz to 5.85 GHz • 802.11b/g: 2.400 GHz to 2.4835 GHz (dependent on country) • 802.11n: 2.400 GHz to 5.00 GHz
Channel Number	Displays the transmit and receive channel.
Network Authentication	Displays Open, Shared, WPA*-Personal, WPA2*-Personal, WPA-Enterprise and WPA2-Enterprise. Displays the authentication used by the currently used profile. See Security Overview for more information.
Data Encryption	Displays None, WEP, TKIP or AES-CCMP. See Security Overview for more information.

802.1X Authentication Type	Displays None, EAP-SIM, TLS, TTLS, PEAP, LEAP, or EAP-FAST. See Security Overview for more information.
802.1X Authentication Protocol	Displays None, PAP, GTC, CHAP, MS-CHAP, MS-CHAP-V2 or TLS. See Security Overview for more information.
CCX Version	Version of the Cisco Compatible Extensions on this wireless connection.
Current Tx Power	The power level at which the WiFi adapter is currently transmitting, in milliwatts.
Supported Power Levels	These are the power levels that the WiFi adapter is capable of transmitting. This information is presented in a range and is dependent on the adapter.
Access Point MAC Address	The Media Access Control (MAC) address for the associated access point.
Mandatory Access Point	Displays None, if not enabled. If enabled, from the Mandatory Access Point setting, the access point MAC address is displayed. This option directs the WiFi adapter to connect to an access point that uses a specific MAC address (48-bit 12 hexadecimal digits, for example, 00:06:25:0E:9D:84).
AP Name	The name of the access point. This name is set by the person configuring the access point and is typically limited to 32 characters. **NOTE**: This parameter is only visible when connected to a Cisco Systems access point.
AP IPV4/IPV6 Address	The Interconnect Protocol address (IPV4 or IPV6) for the access point. IPV6 is the next generation IP address and is backward compatible and is designed to fix data security problems with IPv4. IPv6 increases the address space from 32 to 128 bits, providing for an unlimited number of networks and systems. It also supports quality of service (QoS) parameters for real-time audio and video. **NOTE**: This parameter is only visible when connected to a Cisco Systems access point.

AP Signal Strength	The strength of the signal received from the access point, at the adapter. This value is given in milliwatts (mW) and may actually be in the picowatts range. This value varies, based on the distance between the AP and the adapter, obstacles that may interfere with the signal, and the power level at which the AP is transmitting. **NOTE**: This parameter is only visible when connected to a Cisco Systems access point.
AP Noise Level	The radio frequency (RF) noise level present in the environment that will tend to interfere with the signal from the access point. RF noise comes from natural and electrical sources. **NOTE**: This parameter is only visible when connected to a Cisco Systems access point.
Repair	Renews the IP Address. If you have trouble accessing the network, verify if the IP address is valid. If it is 0.0.0.0 or 169.x.x.x then it is probably not valid. If your network is set up for automatic network address assignment, then click **Repair** and request a new IP address.
Close	Closes the page.
Help?	Provides help information for this page.

[Back to Top](#)

[Back to Contents](#)

Back to Contents

Turn WiFi Radio On or Off

To switch the wireless radio on or off, use one of the following methods:

- The optional hardware radio switch on your computer
- Intel(R) PROSet/Wireless WiFi Connection Utility
- Microsoft Windows

NOTE: When your computer is switched on, the radio is constantly transmitting signals. In certain situations, as in an airplane, signals from the radio may cause interference. Use the following methods if you need to turn off the radio and use your notebook without emitting radio signals.

Use the Optional Computer Radio on or off Switch

If your computer has an external switch installed, use it to switch the radio on or off. See the computer manufacturer's documentation for more information about this switch. If you have Intel PROSet/Wireless WiFi software installed, the current state of the radio displays in the WiFi connection utility main window and on the Taskbar.

Use Intel PROSet/Wireless WiFi to Switch the Radio on or off

From Intel PROSet/Wireless WiFi software, the radio can be switched on or off. The status icon on Intel PROSet/Wireless WiFi displays the current state of the radio.

From the Intel PROSet/Wireless WiFi main Window, click **WiFi On** / **WiFi Off** to toggle the radio on or off.

Switch the radio on or off from the Taskbar Icon

To switch the radio on or off, click the Taskbar icon and select **WiFi On** / **WiFi Off**.

Use Windows to turn on or off the Radio

The radio can be turned off using Windows.

NOTE: If you turned off the radio from Microsoft Windows, then you must use Microsoft Windows to turn the radio on. You cannot use a hardware switch or the WiFi connection utility to enable the radio if the radio has been turned off using Windows.

Windows XP

1. At the Start Menu, click **Connect to**. Right click **Wireless Network Connection** and select **Disable**.
2. Or if you have more than one WiFi adapter, at the Start Menu, click **Connect to** > **Show all connections**. Right click the desired adapter and select **Disable**.

You can use the same method to turn the radio back on.

Back to Top

Back to Contents

Back to Contents

Taskbar Icon

Taskbar Menu Options

The Intel(R) PROSet/Wireless WiFi Connection Utility status icon displays on the Taskbar located in the lower right corner of your Windows desktop. This icon looks like this: 

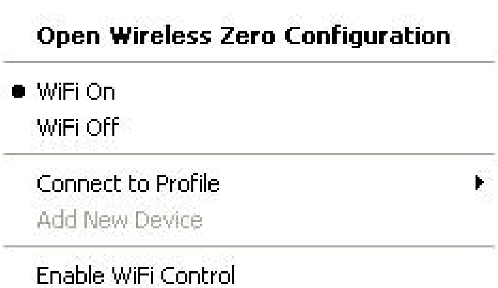
Right-click the status icon to display the menu options.

If the WiFi connection utility is managing your WiFi connections, then the following menu options appear.



Name	Description
Configure WiFi...	Click to open Intel PROSet/Wireless WiFi and configure your WiFi connections.
WiFi On / WiFi Off	Click to turn on or off the Intel WiFi adapter. If you are currently connected to a wireless network and you click WiFi Off, your wireless network connection will be closed.
Connect to Profile	Displays the current profiles in the Profiles list. Click on a profile to connect to it.
Add New Device	This command lets you add a new device (for example, a laptop) using Wi-Fi Protected Setup*. The availability of this command on your computer means that your computer is already configured as a Wi-Fi Protected Setup registrar (using the WiFi connection utility). See Add an New Device.

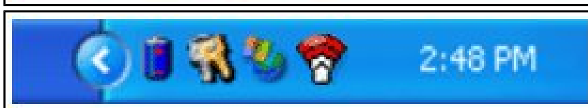
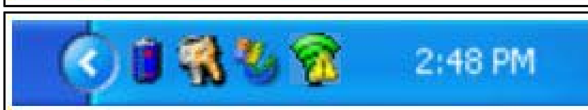
If Windows Zero Configuration manager is managing your WiFi connections, then the following menu options appear.

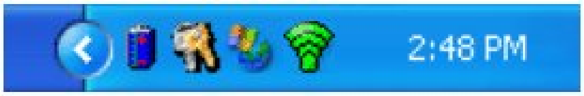


Name	Description
Open Wireless Zero Configuration	Click to open Windows Zero Configuration, the wireless connections manager provided by Windows*. Only available if you have selected **Use Windows to manage WiFi** at the Intel(R) PROSet/Wireless WiFi Connection Utility, Advanced menu.
Configure WiFi	Click to open Intel(R) PROSet/Wireless WiFi Connection Utility and configure your WiFi connections.
WiFi On / WiFi Off	Click to turn on or off the Intel WiFi adapter. If you are currently connected to a wireless network and you click WiFi Off, your wireless network connection will be closed.
Connect to Profile	Displays the current profiles in the Profiles list. Click on a profile to connect to it.
Add New Device	This command lets you add a new device (for example, a laptop) using Wi-Fi Protected Setup*. The availability of this command on your computer means that your computer is already configured as a Wi-Fi Protected Setup registrar (using the WiFi connection utility). See [Add an New Device]().
Enable WiFi Control	Click to assign management of your WiFi wireless connections to the WiFi connection utility. Wireless Zero Configuration manager will no longer manage your connections. If you want to assign management of your WiFi wireless connections back to Wireless Zero Configuration manager, open the Intel(R) PROSet/Wireless WiFi software, and under the Advanced menu, click **Use Windows to Manage WiFi**.

Taskbar Icons

The Taskbar icon  provides visual indication of the current wireless connection state. The connection status icon is located on the lower right corner of your Windows desktop. The Taskbar icon can be set to display or be hidden in the Tools Menu [Application Settings]().

Name	Description
	**WiFi Off** : The WiFi adapter is off. The wireless device does not transmit or receive while it is off. Click **WiFi On** to enable the adapter. The icon is white and static.
	**Searching for WiFi networks**: The WiFi adapter searches for any available WiFi networks. The icon is white with animation.
	**No WiFi networks found**: There are no available WiFi networks found. Intel PROSet/Wireless WiFi periodically scans for available networks. If you want to force a scan, double-click the icon to launch Intel PROSet/Wireless and click **Refresh**. The icon is red.
	**Wireless network found**: An available wireless network is found. Double-click the icon to display the Wireless Networks list. Select the network. Click **Connect**. The icon is yellow.
	**Authentication failed**: Unable to authenticate with wireless network. The icon is green with a yellow warning triangle.
	**Connecting to a wireless network**: Flashes while an IP address is being obtained or if an error occurs.

	**Connected to a wireless network**: Connected to a wireless network. Tool tip displays network name, speed, signal quality and IP address. The icon is green with waves that reflect signal quality. The more waves, the better the signal quality.

Tool Tips and Desktop Alerts

The Tool Tips and Desktop Alerts provide feedback and interaction. To display Tool Tips, move your mouse pointer over the icon. Desktop alerts are displayed when your wireless network changes state. For example, if you are out of range of any WiFi networks, a desktop alert is displayed when you come into range.

Select **Show Information Notifications** in the Application Settings to enable desktop alerts.

Tool Tips

Tool tips display when the mouse pointer rolls over the icon. The tool tips display text for each of the connection states.



Desktop Alerts

When user action is required, a desktop alert displays. If you click the alert, then an appropriate action is taken. For example when WiFi networks are found, the following alert displays:



Action: Click the desktop alert to connect to a network in the WiFi Networks list.

Once connected, the alert displays the wireless network that you are connected to, the speed of the connection, signal quality and IP address.



Desktop alerts are also used to indicate if there is a connection problem. Click the alert to open the Intel(R) Wireless Troubleshooter.



Start Intel PROSet/Wireless WiFi from Taskbar

To start Intel(R) PROSet/Wireless WiFi software:

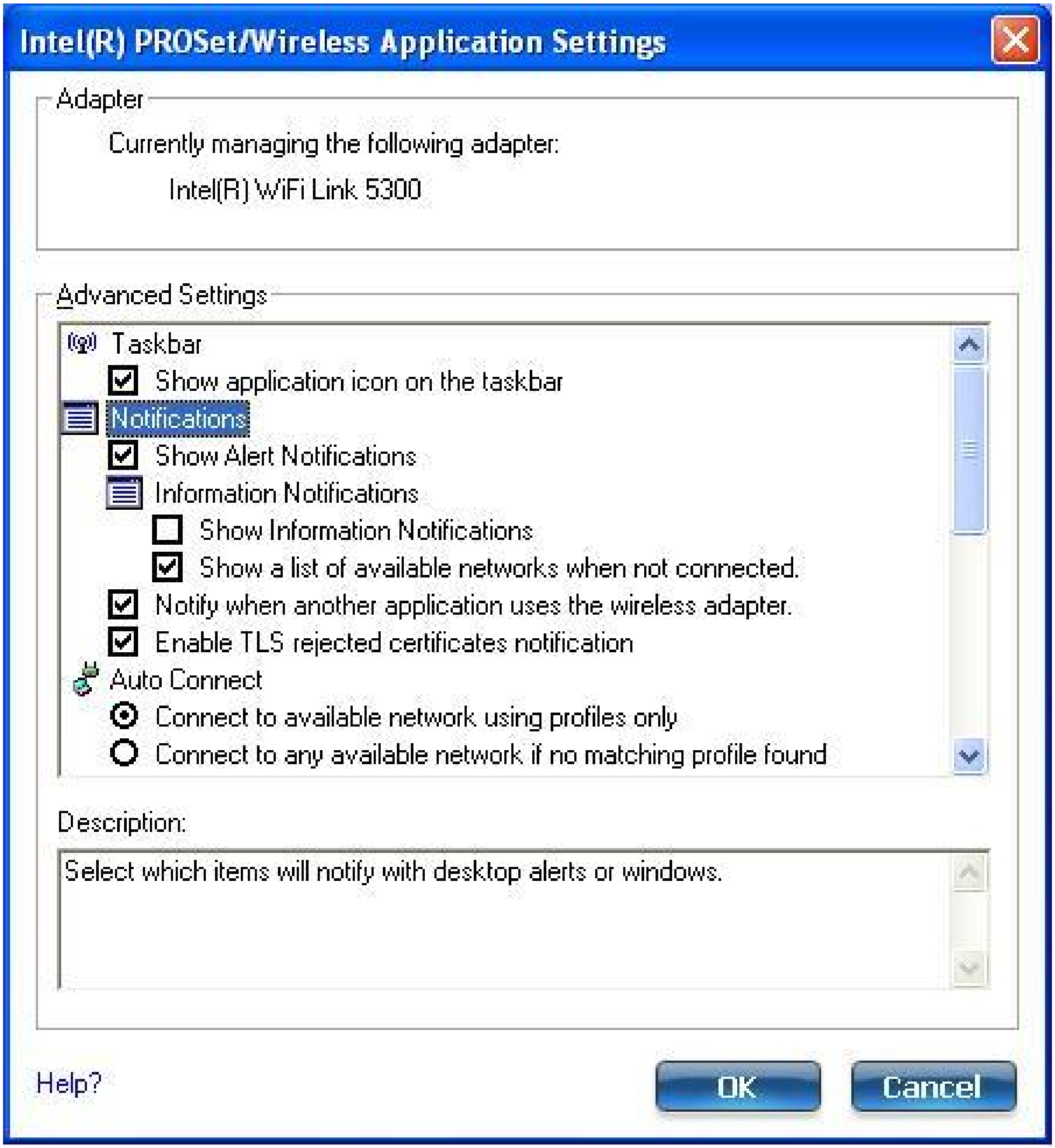
- Double-click the Taskbar icon  located in the lower right corner of your Windows desktop, or
- Right-click the Taskbar icon , and select **Configure WiFi** .

[Back to Top](#)

[Back to Contents](#)

Back to Contents

Application Settings (Tools menu)



The Application Settings control the behavior of the Intel(R) PROSet/Wireless WiFi Connection Utility.

Application Settings Description

Name	Description
Adapter	Lists the network adapter. It may be any one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN • Intel(R) Wireless WiFi Link 4965AG_ • Intel(R) PRO/Wireless 3945ABG Network Connection • Intel(R) PRO/Wireless 2915ABG Network Connection • Intel(R) PRO/Wireless 2200BG Network Connection
Advanced Settings: The following settings control how the WiFi connection utility behaves and displays information.	
Taskbar	**Show application icon on the taskbar**: Select to display the Taskbar status icon. This icon resides on the Windows Taskbar (Notification Area). This icon provides the status of your wireless connection. Clear to not display the Taskbar status icon. The Taskbar Status Icon provides several functions: • Visual feedback for the connection state and wireless activity of your wireless network. The icon changes color and animation for different wireless activity. See Taskbar Icons for more information. • **Menu**: A menu is displayed when you right-click the icon. From this menu you perform tasks such as turn the radio on or off or launch the WiFi connection utility. See: Taskbar Menu Options for more information. • Tool tips and desktop alerts. See: Tool Tips and Desktop Alerts for more information.

Notifications	**Show Alert Notifications**: Select to display desktop alerts next to the taskbar icon. When your action is required, a message displays. Only events of high importance trigger a desktop alert. If the desktop alert is selected, then the appropriate action is taken. Clear to not display desktop alerts. See Tool Tips and Desktop Alerts for more information. Select one of the following options: **Information Notifications**: These desktop alerts are of lower importance. They do not require your interaction but can greatly improve the wireless experience. • **Show Information Notifications**: Selected by default. All informational desktop alerts are displayed next to the taskbar status icon. These desktop alerts improve your wireless experience with notifications when available wireless networks are within range. They also inform you when a wireless connection has been made or has been lost. See Tool Tips and Desktop Alerts for more information. • **Show a list of available networks when not connected**: When **Show Information Notifications** is cleared, you can select this item. When the desktop alerts are disabled, this option lets you continue to be notified of available networks when the WiFi adapter is not connected. **Notify when another application uses the WiFi adapter**: When selected, a message is displayed when other applications are trying to manage your WiFi adapter. This is helpful if you use software provided by a hotspot location (coffee shop, airport terminal). To take advantage of the WiFi connection utility features, disable this software when you leave the hotspot. **Enable TLS rejected certificates notification**: Select if you want a warning issued when a PEAP-TLS certificate is rejected by the authentication server. See Enterprise Security and Set up a Client with TLS Network Authentication for more information.

Auto Connect	**Connect to available network using profiles only**: (Default) Connect the WiFi adapter to an available network with a matching profile from the Profiles List. If no matching profile is found, you are notified (see Notifications). The wireless device remains disconnected until a matching profile is found or you configure a new matching profile. **Connect to any available network if no matching profile found**: Select to connect to a network automatically if you have not configured a profile and are at a location that has an open, unsecured wireless network. **NOTE**: Open networks have no security. You would need to provide your own security for this wireless connection. One way to secure an open wireless connection is with Virtual Private Networking (VPN) software. **Connect to any network based on profiles only (Cisco mode)**: Select to try every profile in preferred order. This signifies that you are in the vicinity of an access point which has more than one SSID but only advertises one. **Do not automatically connect. User will connect manually**: Select to turn off automatic connection.
Manage Exclusions	**Enable automatic exclude list feature**: Select to enable the automatic exclude list feature. This feature provides a way to exclude access points from automatic connection. See Manage Exclusions for more information. **Enable manual exclude list feature**: Select to enable the manual exclude list feature. This feature provides a way to exclude networks from automatic connection. See Manage Exclusions for more information.
WiFi Networks list	**Show column sort headers**: Select to display the column names in the WiFi Networks list. Click a column header to sort the column in either ascending or descending order.

Shared Folder Notification	File and printer sharing enables other computers on a network to access resources on your computer. You should be cautious when you use your wireless notebook computer with file and printer sharing enabled. Use this feature to receive notifications when you connect to a wireless network with shared folders that meet one of the following conditions: • The Microsoft Windows firewall is disabled • File and Printer Sharing are enabled as an exception to the Microsoft Windows firewall settings. **Unshare shared folders automatically when connected to an unsecured network**. Select to unshare shared folders automatically, each time you connect to an unsecured network. This feature provides some additionally security. **Disable this notification** Select to maintain your current shared folder settings each time you connect to an open, unsecured network. **Notify when connected to an unsecured network**. Select to receive notification each time you are connected to an open, unsecured network.
Device to Device (ad hoc) Network Notification	Receive alerts dependent on the following settings when connected to an ad hoc network. You are alerted every two minutes, with a maximum of five alerts. **Notify when no peers have joined the ad hoc network** Select to receive notification if no peers join the ad hoc network. **Notify when all peers leave the ad hoc network** Select to receive an alert when all the peers leave the ad hoc network.

Network Name (SSID) Notification	Notifies you when the default network name (SSID) is used to connect to a network. Common examples of pre-defined, default network names are: wireless, WLAN, linksys, default. Connecting to an access point that has the default network name (SSID) can be a security problem. This access point usually uses all the default security and, management settings (for example, Open authentication; default IP address, user name, or password). If this is a personal network, change the network name and security settings to improve the security of the network. **Notify when connected to a network with the default SSID name** Select to receive an alert when connected to a network with the default network name.
WiFi Settings	**Disable WiFi scanning when associated**: This setting disables scanning for additional WiFi access points after the adapter connects to an access point (network). Disabling scanning when already connected can improve the connection performance.
Wi-Fi Protected Setup*	**Enable device registration** Turn this on to let the computer act as an external registrar. In this capacity, the computer can set up an unconfigured access point or join a configured access point. After the access point has been configured, the computer, as an external registrar, can add new computers (enrollees) to the network. Default state is OFF. Turn **Enable device registration** off to let the computer detect and connect to a network as an enrollee. **Notify when Wi-Fi Protected Setup access points are within range of your computer** Turn to on to let you know when an access point equipped with Wi-Fi Protected Setup* is within range of your computer. This is necessary if you want to enroll (connect) this computer to the access point. Default state is On.
OK	Saves settings and return to the previous page.
Cancel	Closes and cancels changes.

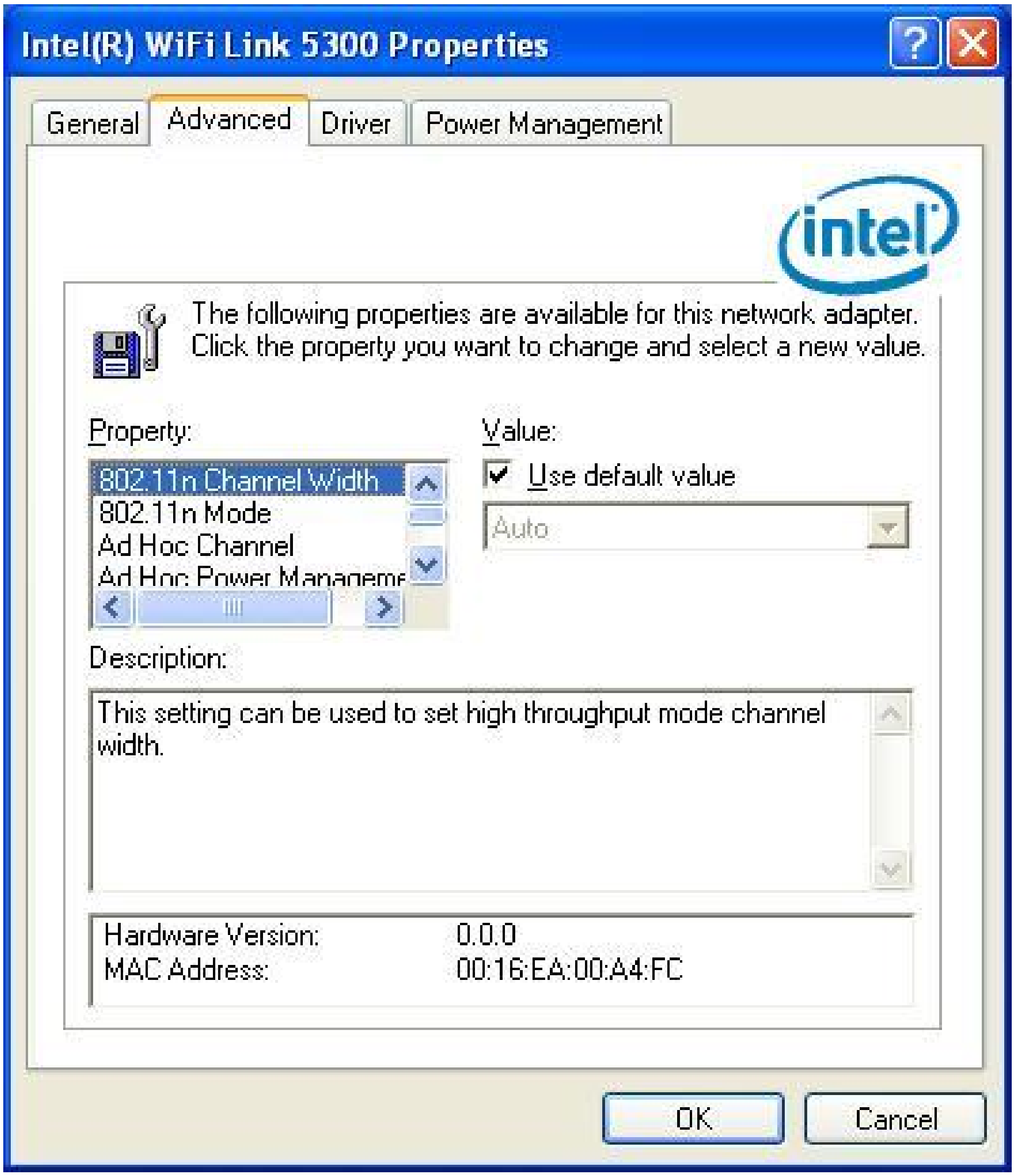
Help?	Provides help information for this page.

[Back to Top](#)

[Back to Contents](#)

Back to Contents

Adapter Settings (Advanced tab)



The Adapter Settings, advanced tab, displays the device properties for the WiFi adapter installed on your computer.

It may be one of the following network connection WiFi adapters:

- Intel(R) WiMAX/WiFi Link 5350

- Intel(R) WiMAX/WiFi Link 5150
- Intel(R) WiFi Link 5300
- Intel(R) WiFi Link 5100
- Intel(R) Wireless WiFi Link 4965AGN
- Intel(R) Wireless WiFi Link 4965AG_
- Intel(R) PRO/Wireless 3945ABG Network Connection
- Intel(R) PRO/Wireless 2915ABG Network Connection
- Intel(R) PRO/Wireless 2200BG Network Connection.

For Windows XP* users, to see the WiFi adapter settings, on the Advanced Menu click **Adapter Settings**. Select the Advanced tab.

WiFi adapter Settings Description

Name	**Description**
802.11n Channel Width (2.4 GHz)	Set high throughput channel width to maximize performance. Set the channel width to **Auto** or **20MHz**. **Auto** is the default setting. Use 20MHz if 802.11n channels are restricted. **NOTE**: This setting is available only if the WiFi adapter is one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN
802.11n Channel Width (5.2 GHz)	Set high throughput channel width to maximize performance. Set the channel width to **Auto** or **20MHz**. **Auto** is the default setting. Use 20MHz if 802.11n channels are restricted. **NOTE**: This setting is available only if the WiFi adapter is one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN

802.11n Mode	The 802.11n standard builds on previous 802.11 standards by adding multiple-input multiple-output (MIMO). MIMO increases data throughput to improve transfer rate. Select **Enabled** or **Disabled** to set the 802.11n mode of the WiFi adapter. Enabled is the default setting. An administrator can enable or disable support for high throughput mode to reduce power-consumption or conflicts with other bands or compatibility issues. **NOTE**: This setting is available only if the WiFi adapter is one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN **NOTE**: To achieve transfer rates greater than 54 Mbps on 802.11n connections, WPA2-AES security must be selected. No security (**None**) can be selected to enable network setup and troubleshooting.
Ad Hoc Channel	Unless the other computers in the ad hoc network use a different channel from the default channel, there is no need to change the channel. **Value**: Select the permitted operating channel from the list. • **802.11b/g**: Select this option when 802.11b and 802.11g (2.4 GHz) ad hoc band frequency is used. • **802.11a**: Select this option when 802.11a (5 GHz) ad hoc band frequency is used. **NOTE**: When an 802.11a channel is not displayed, initiating ad hoc networks is not supported for 802.11a channels.

Ad Hoc Power Management	Set power saving features for device to device (ad hoc) networks. **Disable**: Select when connecting to ad hoc networks that contain stations that do not support ad hoc power management **Maximum Power Savings**: Select to optimize battery life. **Noisy Environment**: Select to optimize performance or connecting with multiple clients. **NOTE**: This setting is only available if the WiFi adapter is one of the following: - Intel(R) WiMAX/WiFi Link 5350 - Intel(R) WiMAX/WiFi Link 5150 - Intel(R) WiFi Link 5300 - Intel(R) WiFi Link 5100 - Intel(R) Wireless WiFi Link 4965AGN - Intel(R) PRO/Wireless 3945ABG
Ad Hoc QoS Mode	Quality of Service (QoS) control in ad hoc networks. QoS provides prioritization of traffic from the access point over a wireless LAN based on traffic classification. WMM (Wi-Fi Multimedia) is the QoS certification of the Wi-Fi Alliance (WFA). When WMM is enabled, the WiFi adapter uses WMM to support priority tagging and queuing capabilities for Wi-Fi networks. **WMM Enabled** (Default) **WMM Disabled** **NOTE**: This setting is only available if the WiFi adapter is one of the following: - Intel(R) WiMAX/WiFi Link 5350 - Intel(R) WiMAX/WiFi Link 5150 - Intel(R) WiFi Link 5300 - Intel(R) WiFi Link 5100 - Intel(R) Wireless WiFi Link 4965AGN - Intel(R) PRO/Wireless 3945ABG

Fat Channel Intolerant	This setting communicates to surrounding networks that this WiFi adapter is not tolerant of 40MHz channels in the 2.4GHz band. The default setting is for this to be turned off (disabled), so that the adapter does not send this notification. **NOTE**: This setting is available only if the WiFi adapter is one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN **NOTE**: This setting is only available to the user and is *not available* for export in an administrator package.
HD Mode	In a wireless network environment where several access points are nearby, this feature will reduce interference and improve your wireless connection. The default setting is for this to be turned off (disabled). **NOTE**: This setting is available only if the WiFi adapter is one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN
Mixed mode protection	Use to avoid data collisions in a mixed 802.11b and 802.11g environment. Request to Send/Clear to Send (RTS/CTS) should be used in an environment where clients may not hear each other. CTS-to-self can be used to gain more throughput in an environment where clients are in close proximity and can hear each other.

Power Management	Lets you select a balance between power consumption and WiFi adapter performance. The WiFi adapter power settings slider sets a balance between the computer's power source and the battery. • **Use default value**: (Default) Power settings are based on the computer's power source. • **Manual**: Adjust the slider for the desired setting. Use the lowest setting for maximum battery life. Use the highest setting for maximum performance. **NOTE**: Power consumption savings vary based on Network (Infrastructure) settings.
Preamble Mode	Changes the preamble length setting received by the access point during an initial connection. Always use **Auto Tx Preamble** to provide optimal network throughput. **Auto Tx Preamble** allows automatic preamble detection. If supported, short preamble should be used. If not, use **Long Tx Preamble**. **NOTE:** This setting is only available if the adapter is an Intel(R) PRO/Wireless 2915ABG Network Connection or an Intel(R) PRO/Wireless 2200BG Network Connection.
Roaming Aggressiveness	This setting lets you define how aggressively your wireless client roams to improve connection to an access point. • **Default**: Balanced setting between not roaming and performance. • **Lowest**: Your wireless client will not roam. Only significant link quality degradation causes it to roam to another access point. • **Highest**: Your wireless client continuously tracks the link quality. If any degradation occurs, it tries to find and roam to a better access point.

Throughput Enhancement	Changes the value of the Packet Burst Control. • **Enable**: Select to enable throughput enhancement. • **Disable**: (Default) Select to disable throughput enhancement.
Transmit Power	**Default Setting**: Highest power setting. **Lowest: Minimum Coverage**.: Set the adapter to the lowest transmit power. Enables you to expand the number of coverage areas or confine a coverage area. Reduces the coverage area in high traffic areas to improve overall transmission quality and avoids congestion and interference with other devices. **Highest: Maximum Coverage**: Set the adapter to a maximum transmit power level. Select for maximum performance and range in environments with limited additional WiFi radio devices. **NOTE**: The optimal setting is for a user to always set the transmit power at the lowest possible level that is still compatible with the quality of their communication. This allows the maximum number of wireless devices to operate in dense areas and reduce interference with other devices that it shares the same radio spectrum with. **NOTE**: This setting takes effect when either Network (Infrastructure) or Device to Device (ad hoc) mode is used.

Wireless Mode	Select which mode to use for connection to a wireless network: • **802.11a only**: Connect the wireless WiFi adapter to 802.11a networks only. • **802.11b only**: Connect the wireless WiFi adapter to 802.11b networks only. • **802.11g only**: Connect the wireless WiFi adapter to 802.11g networks only. • **802.11a and 802.11g**: Connect the WiFi adapter to 802.11a and 802.11g networks only. • **802.11b and 802.11g**: Connect the WiFi adapter to 802.11b and 802.11g networks only. • **802.11a, 802.11b, and 802.11g**: (Default) - Connect to either 802.11a, 802.11b or 802.11g wireless networks. **NOTE**: These wireless modes (Modulation type) determine the discovered access points displayed in the WiFi Networks list
OK	Saves settings and returns to the previous page.
Cancel	Closes and cancels any changes.

Microsoft Windows* Advanced Options (Adapter Settings)

To access the Windows XP* Advanced options:

1. Start Windows and log on with administrative privileges.
2. From your desktop, right-click **My Computer** and click **Properties**.
3. Click the **Hardware** tab.
4. Click **Device Manager**.
5. Double-click **Network adapters**.
6. Right-click the name of the installed WiFi adapter that is in use.
7. Click **Properties**.
8. Select the **Advanced** tab.
9. Select the **Property** you want (for example, Mixed Mode Protection, Power Management).
10. To select a new value or setting, click **Use default value** to clear the checkbox. Then select a new value or setting. To return to the default value, click the **Use default value** checkbox. (The **Use default value** box is not present for all properties, for example, Ad Hoc Channel. In this case, simply select the setting you want.)
11. To save your settings and exit the window, click **OK**.

Back to Top

Back to Contents

Trademarks and Disclaimers

Back to Contents

Wireless Network Overview

About Wireless Networks

A Wireless Local Area Network (WLAN) connects computers without network cables. Instead, computers use radio communications to send data between each other. In a WLAN, a radio communications device called an access point or wireless router connects network computers and provides Internet or network access. You can communicate directly with other wireless computers, or connect to an existing network through a wireless access point.

When you set up your WiFi adapter, you select the operating mode for the kind of wireless network you want. You can use your Intel(R) PRO/Wireless Network Connection adapter to connect to other similar wireless devices that comply with the 802.11 standard for wireless networking. In this Help, a wireless network is also referred to as a WiFi network.

What do I need to Set up a Wireless Network?

The most common type of wireless network is an infrastructure network. To set up an infrastructure network, you need the following:

- A wireless router.
- A wireless network adapter for each computer that you want to connect to the

wireless network.
- If you want internet access for your WLAN, you also need broadband internet service such as cable or DSL. This includes a broadband modem.

Wireless Networking Basics

What is a Wireless Network Management Utility?

The WiFi connection utility is a wireless network management utility. It helps you manage your wireless connections. It can help you initially set up your wireless connections and then easily manager those connections, opening and closing connections and managing security as required. Some computers also ship with Microsoft Windows Zero Configuration, which is another wireless network management utility, and you should not use both of these tools. This is because network settings you create with one utility are not applied if the other utility is managing wireless connections. We recommend that you pick one tool to manage wireless connections, and stay with that.

See Use Microsoft Windows* to Manage WiFi* and also see Get Connected.

Network Name (SSID)

Every wireless local area network (WLAN) uses a unique network name to identify the network. This name is also called the Service Set Identifier (SSID). When you set up your WiFi adapter, you specify the SSID. If you want to connect to an existing WLAN, you must use the name for that network. If you set up your own WLAN, you can make up your own name and use it on each computer. The name can be up to 32 characters long and contain letters and numbers. The SSID or network name is assigned at the access point or wireless router.

Profiles

A profile is used to manage your computer's connection to a WLAN. A profile is a collection of settings that determines how your computer connects to the WLAN. These settings (the profile) are saved on your computer and are used each time you connect to that WLAN. The profile includes all of the network information and security settings. Different profiles are created for different WLANs. For your computer, each WLAN will have its own profile to manage connection to that WLAN. Using the WiFi connection utility, the profiles for your computer are displayed in the Profiles list. From the WiFi connection utility main window you can create, edit, and remove profiles.

Security

Some WLANs are open or unsecure networks, and some are secure networks. A secure WLAN limits who can access the network. There are different levels methods of security. The

WiFi connection utility can easily help you set up a security method for your WLAN.

Common security methods for WLANs use keys or passwords, where the computer requesting access must provide the key or password to get access. WLANs can also use encryption to encode the data. With encryption, before a computer transmits data it uses a secret encryption key to scramble the data. The receiving computer uses this same key to unscramble the data. If you connect to an existing network, use the encryption key provided by the administrator of the wireless network. If you set up your own network, you can make up your own key and use it on each computer. The WiFi connection utility can help you do this. The security method used by your computer to get WLAN access is stored in the profile. See Security for more helpful information.

Identify a Wireless Network

Depending on the size and components of a wireless network, there are different ways to identify a wireless network:

- **The Network Name or Service Set Identifier (SSID)**: Identifies a wireless network. All wireless devices on the network must use the same SSID. This is probably the most common method.
- **Basic Service Set (BSS)**: Consists of two or more wireless nodes, or stations, which have recognized each other and have established communications.
- **Broadcast SSID**: An access point can respond to computers sending probe packets with the broadcast SSID. If this feature is enabled on the access point, any wireless user can associate with the access point by using a blank (null) SSID.
- **Basic Service Set Identifier (BSSID)**: A unique identifier for each wireless device. The BSSID is the Ethernet MAC address of the device.
- **Extended Service Set Identifier (ESSID)**: A special case of SSID used to identify a wireless network that includes access points.
- **Independent Basic Service Set (IBSS)**: A mode of operation in an 802.11 system that allows direct communication between 802.11 devices without the need to set up a communication session with an access point.
- **Independent Basic Service Set Identifier (IBSSID)**: A special case of SSID used to identify a network of wireless computers configured to communicate directly with one another without using an access point.

Select a Wireless Network Mode

Wireless networks can operate with or without access points, depending on the number of users in the network. Infrastructure mode uses access points to allow wireless computers to send and receive information. Wireless computers transmit to the access point, the access point receives the information and rebroadcasts it to other computers. The access point can also connect to a wired network or to the Internet. Multiple access points can work together to provide coverage over a wide area.

Device-to-Device mode, also called ad hoc mode, works without access points and allows

wireless computers to send information directly to other wireless computers. You can use Device-to-Device mode to network computers in a home or small office or to set up a temporary wireless network for a meeting.

How do I turn my Radio on and off?

You will need to turn the WiFi adapter radio off (and on) on different occasions. For example, you may be required to turn the radio off when boarding an airplane. You can also turn it off to conserve battery power.

There are three methods to turn the radio on and off:

- Using the wireless radio hardware switch (may not be present on all computers).
- Using the **WiFi On** / **WiFi Off** button in the WiFi connection utility.
- Using Windows.

Remember that to connect to wireless networks, the wireless radio needs to be turned back on. If you are unable to connect to a wireless network, verify that your radio is turned on at *both* the hardware switch *and* the **WiFi On** / **WiFi Off** button in the WiFi connection utility.

See Turn the Radio on or off for more information.

Back to Top

Back to Contents

Back to Contents

Security Overview

This section describes the various security methods used to help protect WiFi networks.

Protecting Your WiFi Network

Your wireless network, if left unprotected, is vulnerable to access from other computers. You can easily protect your home and small business network from nearly all forms of unauthorized access with the security methods described in this section.

Authentication

Authentication is the process of identifying and approving a request from a client (usually a laptop) to access a network at a network access point. Once authentication is completed and access is granted, the client has access to the network.

Encryption

You can select encryption algorithms to encrypt the information and data that is sent across your wireless network. Only computers equipped with pre-shared keys can encrypt and decrypt the data being transmitted. Encryption keys are available with two levels of security, 64-bit and 128-bit. Use 128-bit keys for greater security.

SSID Broadcasting

A simple way to improve network security is to set your network access point to *not broadcast* the Service Set Identifier (SSID). The SSID is needed to gain access. Only those computers with knowledge of the SSID can access the network. (This is *not* set at the adapter using the Intel(R) PROSet/Wireless WiFi Connection Utility, it is set at the access point.)

Personal Security Methods

Open and Shared Network Authentication

IEEE 802.11 supports two types of network authentication methods: Open System and Shared Key.

- When *open* authentication is used, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management request that contains the identity of the sending station. The receiving station or access point grants any request for authentication. Open authentication allows any device to gain network access. *If no encryption is enabled on the network, any device that knows the Service Set Identifier (SSID) of the access point can gain access to the network.*
- When *shared key* authentication is used, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel. You can share this secret key via a wired Ethernet connection, or by physically using a USB memory stick or CD. Shared key authentication requires that the client configure a static WEP key. The client access is granted only if it passes a challenge-based authentication.

WEP

Wired Equivalent Privacy (WEP) uses encryption to help prevent unauthorized reception of wireless data. WEP uses an *encryption key* to encrypt data before transmitting it. Only computers that use the same encryption key can access the network and decrypt the data transmitted by other computers. WEP encryption provides for two levels of security, using a 64-bit key (sometimes referred to as 40-bit) or a 128-bit key (also known as 104-bit). For stronger security, you should use a 128-bit key. If you use encryption, all wireless devices on your wireless network must use the same encryption keys.

With WEP data encryption, a wireless station can be configured with up to four keys (the key index values are 1, 2, 3, and 4). When an access point (AP) or a wireless station transmits an encrypted message that uses a key stored in a specific key index, the transmitted message indicates the key index that was used to encrypt the message body. The receiving AP or wireless station can then retrieve the key that is stored at the key index and use it to decode the encrypted message body

Because the WEP encryption algorithm is *vulnerable* to network attacks, you should consider using WPA-Personal or WPA2-Personal security.

WPA-Personal

WPA-Personal Mode is targeted to home and small business environments. WPA Personal requires manual configuration of a pre-shared key (PSK) on the access point and clients. No authentication server is needed. The same password entered at the access point needs to be used on this computer and all other wireless devices that access the wireless network. Security depends on the strength and secrecy of the password. The longer the password, the stronger the security of the wireless network. If your wireless access point or router supports WPA-Personal and WPA2-Personal then you should enable it on the access point and provide a long, strong password. WPA-Personal makes available the TKIP and AES-CCMP data encryption algorithms.

WPA2-Personal

WPA2-Personal requires manual configuration of a pre-shared key (PSK) on the access point and clients. No authentication server is needed. The same password entered at the access point needs to be used on this computer and all other wireless devices that access the wireless network. Security depends on the strength and secrecy of the password. The longer the password, the stronger the security of the wireless network. WPA2 is an improvement over WPA and implements the full IEEE 802.11i standard. WPA2 is backward compatible with WPA. WPA2-Personal makes available the TKIP and AES-CCMP data encryption algorithms.

NOTE: WPA-Personal and WPA2-Personal are interoperable.

802.1X Authentication (Enterprise Security)

This section describes security common used by larger companies.

Overview

The 802.1X authentication is independent of the 802.11 authentication process. The 802.11 standard provides a framework for various authentication and key-management protocols. There are different 802.1X authentication types and each provides a different approach to authentication, but all employ the same 802.11 protocol and framework for communication between a client and an access point. In most protocols, after completion of the 802.1X authentication process, the client receives a key that it uses for data encryption. See How 802.1X authentication works for more information. With 802.1X authentication, an authentication method is used between the client and a server (for example a Remote Authentication Dial-In User Service (RADIUS) server) connected to the access point. The authentication process uses credentials, such as a user's password, that are *not transmitted* over the wireless network. Most 802.1X types support dynamic per-user, per-session keys to strengthen the key security. The 802.1X authentication benefits from the use of an existing authentication protocol known as the Extensible Authentication Protocol (EAP).

The 802.1X authentication for wireless networks has three main components:

- The authenticator (the access point)
- The supplicant (the client software)
- The authentication server

The 802.1X authentication security initiates an authorization request from the wireless client to the access point, which authenticates the client to an Extensible Authentication Protocol (EAP) compliant RADIUS server. This RADIUS server may authenticate either the user (via passwords or certificates) or the system (by MAC address). In theory, the wireless client is not allowed to join the networks until the transaction is complete. (Not all authentication methods use a RADIUS server. WPA-Personal and WPA2-Personal use a common password that must be entered at the access point and at all devices requesting access to the network.)

There are several authentication algorithms used with 802.1X. Some examples are: EAP-TLS, EAP-TTLS, Protected EAP (PEAP), and EAP Cisco Wireless Light Extensible Authentication Protocol (LEAP). These are all methods for the wireless client to identify itself to the RADIUS server. With RADIUS authentication, user identities are checked against databases. RADIUS constitutes a set of standards that addresses Authentication, Authorization, and Accounting (AAA). RADIUS includes a *proxy* process to validate clients in a multi-server environment. The IEEE 802.1X standard provides a mechanism for controlling

and authenticating access to port-based 802.11 wireless and wired Ethernet networks. Port-based network access control is similar to a switched local area network (LAN) infrastructure that authenticates devices attached to a LAN port and prevents access to that port if the authentication process fails.

What is RADIUS?

RADIUS is the Remote Authentication Dial-In User Service, an Authorization, Authentication, and Accounting (AAA) client-server protocol that is used when a AAA dial-up client logs in or out of a Network Access Server. Typically, a RADIUS server is used by Internet Service Providers (ISP) to perform AAA tasks. AAA phases are described as follows:

- **Authentication phase**: Verifies a user name and password against a local database. After credentials are verified, the authorization process begins.
- **Authorization phase**: Determines whether a request is allowed access to a resource. An IP address is assigned for the dial-up client.
- **Accounting phase**: Collects information on resource usage for the purpose of trend analysis, auditing, session-time billing, or cost allocation.

How 802.1X Authentication Works

Following is a simplified description of how 802.1X authentication works.

1. A client sends a "request to access" message to an access point. The access point requests the identity of the client.
2. The client replies with its identity packet, which is passed along to the authentication server.
3. The authentication server sends an "accept" packet to the access point.
4. The access point places the client port in the authorized state and data traffic is allowed to proceed.

802.1X Features

The following authentication methods are supported on Windows XP:

- 802.1X supplicant protocol support
- Support for the Extensible Authentication Protocol (EAP) - RFC 2284
- Supported Authentication Methods on Windows XP:
    - EAP TLS Authentication Protocol - RFC 2716 and RFC 2246
    - EAP Tunneled TLS (TTLS)
    - Cisco LEAP

- PEAP
- EAP-SIM
- EAP-FAST
- EAP-AKA

Network Authentication

Open

See Open Authentication.

Shared

See Shared Authentication.

WPA-Personal

See WPA-Personal.

WPA2-Personal

See WPA2-Personal.

WPA Enterprise

Enterprise Mode authentication is targeted to corporate or government environments. WPA Enterprise verifies network users through a RADIUS or other authentication server. WPA uses 128-bit encryption keys and dynamic session keys to ensure your wireless network's privacy and enterprise security. An authentication type is selected to match the authentication protocol of the 802.1X server.

WPA2 Enterprise

WPA Enterprise authentication is targeted to corporate or government environments. WPA2 Enterprise verifies network users through a RADIUS or other authentication server. WPA2 uses 128-bit encryption keys and dynamic session keys to ensure your wireless network's privacy and enterprise security. An authentication type is selected to match the authentication protocol of the 802.1X server. Enterprise Mode is targeted to corporate or government environments. WPA2 is an improvement over WPA and implements the full IEEE 802.11i standard.

Data Encryption

AES-CCMP

Advanced Encryption Standard - Counter CBC-MAC Protocol. The new method for privacy protection of wireless transmissions specified in the IEEE 802.11i standard. AES-CCMP provides a stronger encryption method than TKIP. Choose AES-CCMP as the data encryption method whenever strong data protection is important. AES-CCMP is available with WPA/ WPA2 Personal/Enterprise network authentication.

NOTE: Some security solutions may not be supported by your computer's operating system and may require additional software or hardware as well as wireless LAN infrastructure support. Check with your computer manufacturer for details.

TKIP

Temporal Key Integrity Protocol provides per-packet key mixing, a message integrity check, and a rekeying mechanism. TKIP is available with WPA/WPA2 Personal/Enterprise network authentication.

CKIP

See CKIP.

WEP

Wired Equivalent Privacy (WEP) uses encryption to help prevent unauthorized reception of wireless data. WEP uses an *encryption key* to encrypt data before transmitting it. Only computers that use the same encryption key can access the network and decrypt the data transmitted by other computers. Enterprise WEP is not exactly the same as personal WEP, in that you can select **Open** network authentication and then click **Enable 802.1X** and be able to choose from all client authentication types. The selection of authentication types are not available under personal WEP.

Authentication Types

TLS

A type of authentication method using the Extensible Authentication Protocol (EAP) and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates which

use passwords. EAP-TLS authentication supports dynamic WEP key management. The TLS protocol is intended to secure and authenticate communications across a public network through data encryption. The TLS Handshake Protocol allows the server and client to provide mutual authentication and to negotiate an encryption algorithm and cryptographic keys before data is transmitted.

TTLS

These settings define the protocol and the credentials used to authenticate a user. In TTLS (Tunneled Transport Layer Security), the client uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client can use another authentication protocol. Typically, password-based protocols challenge over a non-exposed TLS encrypted channel. TTLS implementations today support all methods defined by EAP, as well as several older methods (PAP, CHAP, MS-CHAP and MS-CHAP-V2). TTLS can easily be extended to work with new protocols by defining new attributes to support new protocols.

PEAP

PEAP is a new Extensible Authentication Protocol (EAP) IEEE 802.1X authentication type designed to take advantage of server-side EAP-Transport Layer Security (EAP-TLS) and to support various authentication methods, including users' passwords, one-time passwords, and Generic Token Cards.

LEAP

A version of Extensible Authentication Protocol (EAP). Light Extensible Authentication Protocol (LEAP) is a proprietary extensible authentication protocol developed by Cisco that provides a challenge-response authentication mechanism and dynamic key assignment.

EAP-SIM

Extensible Authentication Protocol Method for GSM Subscriber Identity (EAP-SIM) is a mechanism for authentication and session key distribution. It uses the Global System for Mobile Communications (GSM) Subscriber Identity Module (SIM). EAP-SIM uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. EAP-SIM requires you to enter a user verification code, or PIN, for communication with the Subscriber Identity Module (SIM) card. A SIM card is a special smart card that is used by Global System for Mobile Communications (GSM) based digital cellular networks. RFC 4186 describes EAP-SIM.

EAP-AKA

EAP-AKA (Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement) is an EAP mechanism for authentication and session key distribution, using the Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (USIM). The USIM card is a special smart card used with cellular networks to validate a given user

with the network.

Authentication Protocols

PAP

Password Authentication Protocol is a two-way handshake protocol designed for use with PPP. Password Authentication Protocol is a plain text password used on older SLIP systems. It is not secure. Only available for TTLS Authentication Type.

CHAP

Challenge Handshake Authentication Protocol is a three-way handshake protocol that is considered more secure than Password Authentication Protocol. Only available for TTLS authentication Type.

MS-CHAP (MD4)

Uses a Microsoft version of RSA Message Digest 4 challenge-and-reply protocol. This only works on Microsoft systems and enables data encryption. To select this authentication method causes all data to be encrypted. Only available for TTLS authentication type.

MS-CHAP-V2

Introduces an additional feature not available with MS-CHAP-V1 or standard CHAP authentication, the change password feature. This feature allows the client to change the account password if the RADIUS server reports that the password has expired. Available for TTLS and PEAP authentication types.

Generic Token Card (GTC)

Carries user specific token cards for authentication. The main feature in GTC is Digital Certificate/Token Card-based authentication. In addition, GTC includes the ability to hide user name identities until the TLS encrypted tunnel is established, which provides additional confidentiality that user names are not being broadcasted during the authentication phase. Only available for PEAP authentication type.

TLS

The TLS protocol is intended to secure and authenticate communications across a public network through data encryption. The TLS Handshake Protocol allows the server and client

to provide mutual authentication and to negotiate an encryption algorithm and cryptographic keys before data is transmitted. Only available for PEAP authentication type.

Cisco Features

Cisco LEAP

Cisco LEAP (Cisco Light EAP) is a server and client 802.1X authentication through a user-supplied logon password. When a wireless access point communicates with a Cisco LEAP-enabled RADIUS (Cisco Secure Access Control Server [ACS]), Cisco LEAP provides access control through mutual authentication between client WiFi adapters and the wireless networks and provides dynamic, individual user encryption keys to help protect the privacy of transmitted data.

Cisco Rogue Access Point Security Feature

The Cisco Rogue access point feature provides security protection from an introduction of a rogue access point that could mimic a legitimate access point on a network in order to extract information about user credentials and authentication protocols that could compromise security. This feature only works with Cisco's LEAP authentication. Standard 802.11 technology does not protect a network from the introduction of a rogue access point. See LEAP Authentication for more information.

802.11b and 802.11g Mixed Environment Protection Protocol

Some access points, for example Cisco 350 or Cisco 1200, support environments in which not all client stations support WEP encryption; this is called Mixed-Cell Mode. When these wireless networks operate in "optional encryption" mode, client stations that join in WEP mode, send all messages encrypted, and stations that use standard mode send all messages unencrypted. These access points broadcast that the network does not use encryption but allow clients that use WEP mode. When "Mixed-Cell" is enabled in a profile, it lets you connect to access points that are configured for "optional encryption."

CKIP

Cisco Key Integrity Protocol (CKIP) is Cisco proprietary security protocol for encryption in 802.11 media. CKIP uses the following features to improve 802.11 security in infrastructure mode:

- Key Permutation (KP)
- Message Sequence Number

NOTE: CKIP is not used with WPA/WPA2 Personal/Enterprise network authentication.

NOTE: CKIP is only supported through the use of the WiFi connection utility on Windows XP.

Fast Roaming (CCKM)

When a wireless LAN is configured for fast reconnection, a LEAP-enabled client device can roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), an access point configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client without perceptible delay in voice or other time-sensitive applications.

Mixed-Cell Mode

Some access points, for example Cisco 350 or Cisco 1200, support environments in which not all client stations support WEP encryption; this is called Mixed-Cell Mode. When these wireless network operate in "optional encryption" mode, client stations that join in WEP mode send all messages encrypted, and stations that use standard mode send all messages unencrypted. These access points broadcast that the network does not use encryption, but allows clients that use WEP mode to join. When Mixed-Cell is enabled in a profile, it lets you connect to access points that are configured for "optional encryption."

Radio Management

When this feature is enabled your WiFi adapter provides radio management information to the Cisco infrastructure. If the Cisco Radio Management utility is used on the infrastructure it configures radio parameters, detects interference and rogue access points.

EAP-FAST

EAP-FAST, like EAP-TTLS and PEAP, uses tunneling to protect traffic. The main difference is that EAP-FAST does not use certificates to authenticate. Provisioning in EAP-FAST is negotiated solely by the client as the first communication exchange when EAP-FAST is requested from the server. If the client does not have a pre-shared secret Protected Access Credential (PAC), it is able to initiate a provisioning EAP-FAST exchange to dynamically obtain one from the server.

EAP-FAST documents two methods to deliver the PAC: manual delivery through an out-of-band secure mechanism and automatic provisioning.

- Manual delivery mechanisms are any delivery mechanism that the administrator of the network considers sufficiently secure.
- Automatic provisioning establishes an encrypted tunnel to protect the authentication of the client and the delivery of the PAC to the client. This mechanism, while not as secure as a manual method may be, is more secure than the authentication method

used in LEAP.

The EAP-FAST method is divided into two parts: provisioning and authentication. The provisioning phase involves the initial delivery of the PAC to the client. This phase only needs to be performed once per client and user.

Back to Top

Back to Contents

Back to Contents

Personal Security

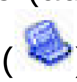
Use Personal Security if you are a home or small business user who can use a variety of simple security procedures to protect your wireless connection. You may want to select from the list of security settings that are easy to configure, for your wireless network. See Personal Security Settings for a description of each of the options. A RADIUS or AAA server is not required.

- Review the Set up Data Encryption and Authentication information to learn about the different security types.
- To add or change the required security settings, click Security Settings for information to set security for the selected wireless network.
- See Profile Management for a description of when to use the Profile Wizard.
- See Security Overview for more information about the different security options for wireless networks.
- If you want to verify the security settings, select a wireless network in the WiFi Networks list. See Network Properties to review the operating mode, authentication level, and data encryption.
- See Enterprise Security to set 802.1X authentication security.

Personal Security Settings

Personal Security Settings Description

Name	Setting

General Settings	Select to open the Personal Security Settings. The security settings that are available are dependent on the Operating Mode selected in the Create WiFi Profile Security Settings. **Device to Device (ad hoc)**: In device to device mode, also called ad hoc mode, wireless computers send information directly to other wireless computers. You can use ad hoc mode to network multiple computers in a home or small office, or to set up a temporary wireless network for a meeting. **NOTE**: Device to Device (ad hoc) networks are identified with a notebook image () in the WiFi Networks and Profiles list. **Network (Infrastructure)**: An infrastructure network consists of one or more access points and one or more computers with WiFi adapters installed. At least one access point should also have a wired connection. For home users, this is usually a broadband or cable network. **NOTE**: Infrastructure networks are identified with an access point image () in the WiFi Networks and Profiles list.
Security Settings	If you are configuring a Device to Device (ad hoc) profile, select one of the following data encryption settings: • None: No authentication required. • WEP-64 bit or WEP-128 bit: A network key or password is used for encryption. If you are configuring a Network (Infrastructure) profile, select: • WPA*-Personal (TKIP) or WPA2*-Personal (TKIP): WPA-Personal uses the Temporal Key Integrity Protocol (TKIP) for data encryption. • WPA-Personal (AES-CCMP) or WPA2-Personal (AES-CCMP): WPA-Personal uses a new method for privacy protection of wireless transmissions specified in the IEEE 802.11i standard.

Advanced button	Click to access the Advanced Settings and configure the following options: • Auto Connect: Select to automatically or manually connect to a profile. • Auto Import: Network administrator can export a profile on another computer. • Band Selection: Select the band to use for this connection profile. • Mandatory Access Point: Select to associate the WiFi adapter with a specific access point. • Password Protection: Select to password protect a profile. • Start Application: Specify a program to be started when a wireless connection is made. • Maintain Connection: Select to remain connected to a user profile after log off.
Back	View the prior page in the Profile Wizard.
OK	Closes the Profile Wizard and saves the profile.
Cancel	Closes the Profile Wizard and cancels any changes made.
Help?	Provides the help information for the current page.

Set up Data Encryption and Authentication

In a home wireless network you can use a variety of simple security procedures to protect your wireless connection. These include:

- Enable Wi-Fi Protected Access (WPA*).
- Change your password.
- Change the network name (SSID).

Wi-Fi Protected Access (WPA) encryption provides protection for your data on the network. WPA uses an encryption key called a Pre-Shared Key (PSK) to encrypt data before transmission. Enter the same password in all of the computers and access point in your home or small business network. Only devices that use the same encryption key can access the network or decrypt the encrypted data transmitted by other computers. The password automatically initiates the Temporal Key Integrity Protocol (TKIP) or AES-CCMP protocol for the data encryption process.

Network Keys

WEP encryption provides two levels of security:

- 64-bit key (sometimes referred to as 40-bit)
- 128-bit key (also known as 104-bit)

For improved security, use a 128-bit key. If you use encryption, all wireless devices on your wireless network must use the same encryption keys.

You can create the key yourself and specify the key length (64-bit or 128-bit) and key index (the location that a specific key is stored). The greater the key length, the more secure the key. When the length of a key is increased by one character, the number of possible keys doubles.

Key Length: 64-bit

> **Pass phrase (64-bit)**: Enter five (5) alphanumeric characters, 0-9, a-z or A-Z.
> **Hex key (64-bit)**: Enter 10 hexadecimal characters, 0-9, A-F.

Key Length: 128-bit

> **Pass phrase (128-bit)**: Enter 13 alphanumeric characters, 0-9, a-z or A-Z.
> **Hex key (128-bit)**: Enter 26 hexadecimal characters, 0-9, A-F.

With WEP data encryption, wireless station can be configured with up to four keys (the key index values are 1, 2, 3, and 4). When an access point or a wireless station transmits an encrypted message that uses a key stored in a specific key index, the transmitted message indicates the key index that was used to encrypt the message body. The receiving access point or wireless station can then retrieve the key that is stored at the key index and use it to decode the encrypted message body.

Set up a Client with Open Authentication and No Data Encryption (None)

CAUTION: Networks using no authentication or encryption are highly vulnerable to access by unauthorized users.

On the Intel(R) PROSet/Wireless WiFi main window, use one of the following methods to connect to a device to device network:

- Double-click a Device to Device (ad hoc) network in the WiFi Networks list.
- Select a Device to Device (ad hoc) network in the WiFi Networks list. Click **Connect**. The Intel(R) PROSet/Wireless WiFi Connection Utility automatically detects the

security settings for the WiFi adapter.

To create a profile for a WiFi network connection with no encryption perform these steps:

1. Click **Profiles** on the WiFi connection utility main window.
2. On the Profiles list, click **Add** to open the **Create WiFi Profile General Settings**.
3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the name of your wireless network.
5. **Operating Mode**: Click **Device to Device (ad hoc)**.
6. Click **Next** to open the **Security Settings**. **Personal Security** is selected by default.
7. **Security Settings**: The default setting is **None**, which indicates that there is no security on this wireless network.
8. Click **OK**. The profile is added to the Profiles list and connects to the wireless network.

Set up a Client with WEP 64-bit or WEP 128-bit Data Encryption

When WEP data encryption is enabled, a network key or password is used for encryption.

A network key is provided for you automatically (for example, it might be provided by your wireless network adapter manufacturer), or you can enter it yourself and specify the key length (64-bit or 128-bit), key format (ASCII characters or hexadecimal digits), and key index (the location where a specific key is stored). The greater the key length, the more secure the key.

To add a network key for an infrastructure network connection:

1. On the WiFi connection utility main window, double-click an infrastructure network in the WiFi Networks list or select the network and click **Connect**.
2. Click **Profiles** to access the Profiles list.
3. Click **Properties** to open the **Create WiFi Profile General Settings**. The Profile name and WiFi Network Name (SSID) display. Network (Infrastructure) should be selected as the Operating Mode.
4. Click **Next** to open the **Security Settings**. **Personal Security** is selected by default.
5. **Security Settings**: The default data encryption setting is **None**, which indicates that there is no security on this wireless network.

To add a password or network key:

1. **Security Settings**: Select either **WEP 64-bit** or **WEP 128-bit** to configure WEP data encryption with a 64-bit or 128-bit key.

   When WEP encryption is enabled on an access point, the WEP key is used to verify access to the network. If the wireless device does not have the correct

WEP key, even though authentication is successful, the device is unable to transmit data through the access point or decrypt data received from the access point.

Name	Description
Password	Enter the Wireless Security Password (Pass phrase) or Encryption Key (WEP key).
Pass phrase (64-bit)	Enter five (5) alphanumeric characters, 0-9, a-z or A-Z.
WEP key (64-bit)	Enter 10 hexadecimal characters, 0-9, A-F.
Pass phrase (128-bit)	Enter 13 alphanumeric characters, 0-9, a-z or A-Z.
WEP key (128-bit)	Enter 26 hexadecimal characters, 0-9, A-F.

2. **Key Index**: Change the Key Index to set up to four passwords.
3. Click **OK** to return to the Profiles list.

To add more than one password:

1. Select the Key Index number: **1, 2, 3,** or **4**.
2. Enter the Wireless Security Password.
3. Select another Key Index number.
4. Enter another Wireless Security Password.
5. Click **OK** to return to the Profiles list.

Set up a Client with WPA*-Personal (TKIP) or WPA2*-Personal (TKIP) Security Settings

WPA* Personal Mode requires manual configuration of a pre-shared key (PSK) on the access point and clients. This PSK authenticates a user's password or identifying code, on both the client station and the access point. The access point performs the authentication. WPA Personal Mode is targeted to home and small business environments.

WPA2* is the second generation of WPA security that provides enterprise and consumer wireless users with a high level of assurance that only authorized users can access their wireless networks. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government users.

NOTE: To achieve transfer rates greater than 54 Mbps on 802.11n connections, WPA2-AES security must be selected. No security (**None**) can be selected to enable network setup and troubleshooting.

To configure a profile with WPA-Personal network authentication and TKIP data encryption:

1. On the WiFi connection utility main window, double-click an infrastructure network in the WiFi Networks list or select the network and click **Connect**.
2. Click **Profiles** to access the Profiles list.
3. Click **Properties** to open the **WiFi Profile Properties General Settings**. The Profile name and WiFi Network Name (SSID) display. Network (Infrastructure) should be selected as the Operating Mode.
4. Click **Next** to open the **Security Settings**.
5. Select **Personal Security**.
6. **Security Settings**: Select **WPA-Personal (TKIP)** to provide security to a small business network or home environment. A password, called a pre-shared key (PSK), is used. The longer the password, the stronger the security of the wireless network.

   If your wireless access point or router supports WPA2-Personal, then you should enable it on the access point and provide a long, strong password. The longer the password, the stronger the security of the wireless network. The same password entered in the access point needs to be used on this computer and all other wireless devices that access the wireless network.

   NOTE: WPA-Personal and WPA2-Personal are interoperable.

7. **Wireless Security Password (Encryption Key)**: Enter a text phrase with eight to 63 characters. Verify that the network key matches the password in the wireless access point.
8. Click **OK** to return to the Profiles list.

Set up a Client with WPA*-Personal (AES-CCMP) or WPA2*-Personal (AES-CCMP) Security Settings

Wi-Fi Protected Access (WPA*) is a security enhancement that strongly increases the level of data protection and access control to a wireless network. WPA enforces 802.1X authentication and key-exchange and only works with dynamic encryption keys. For a home user or small business, WPA-Personal uses either Advanced Encryption Standard - Counter CBC-MAC Protocol (AES-CCMP) or Temporal Key Integrity Protocol (TKIP).

NOTE: To achieve transfer rates greater than 54 Mbps on 802.11n connections, WPA2-AES security must be selected. No security (**None**) can be selected to enable network setup and troubleshooting.

To create a profile with WPA2*-Personal network authentication and AES-CCMP data encryption:

1. On the WiFi connection utility main window, double-click an infrastructure network from the WiFi Networks list or select the network and click **Connect**.
2. If these are being transmitted, the Profile name and WiFi Network Name (SSID) should display on the **General Settings** screen. **Network (Infrastructure)** should be selected as the Operating Mode. Click **Next** to open the **Security Settings**.
3. Select **Personal Security**.
4. **Security Settings**: Select **WPA2-Personal (AES-CCMP)** to provide this level of security in the small network or home environment. It uses a password, also called a pre-shared key (PSK). The longer the password, the stronger the security of the wireless network.

   AES-CCMP (Advanced Encryption Standard - Counter CBC-MAC Protocol) is a newer method for privacy protection of wireless transmissions specified in the IEEE 802.11i standard. AES-CCMP provides a stronger encryption method than TKIP. Choose AES-CCMP as the data encryption method whenever strong data protection is important.

   If your Wireless access point or router supports WPA2-Personal, then you should enable it on the access point and provide a long, strong password. The same password entered into the access point needs to be used on this computer and all other wireless devices that access the wireless network.

   NOTE: WPA-Personal and WPA2-Personal are interoperable.

5. **Password: Wireless Security Password (Encryption Key)**: Enter a text phrase (length is between eight and 63 characters). Verify that the network key used matches the wireless access point key.
6. Click **OK** to return to the Profiles list.

[Back to Top](#)

[Back to Contents](#)

[Trademarks and Disclaimers](#)

Back to Contents

Enterprise Security

From the Security Settings page you can enter the required security settings for the selected wireless network. See Personal Security to set basic WEP or WPA security in a non-enterprise environment (home, small business). See Enterprise Security Settings to set up 802.1X security authentication options.

- Use Enterprise Security if your network environment requires 802.1X authentication.
- 802.1X authentication methods include passwords, certificates and smart cards.
- 802.1X authentication types are: EAP-SIM, EAP-AKA, LEAP, TLS, TTLS, PEAP, EAP-FAST.
- See Profile Management for a description of when the Profile Wizard is launched.
- See Security Overview for more information about the different security options for wireless networks.

Enterprise Security Settings

Enterprise Security Settings Description

Name	Setting
Enterprise Security	Select to open the Enterprise Security settings. The security settings that are available are dependent on the Operating Mode selected: Device to Device (ad hoc) or Network (Infrastructure).

Network Authentication	If you configure a profile for Device to Device (ad hoc) networking, the default setting is Open authentication. If you configure a profile for an infrastructure network, select: • Open: Any wireless station can request authentication. • Shared: Uses an encryption key known only to the receiver and sender of data. • WPA-Personal or WPA2-Personal: Uses a password also called a pre-shared key (PSK). • WPA-Enterprise or WPA2-Enterprise: Use on enterprise networks with an 802.1X RADIUS server. **NOTE**: WPA-Enterprise and WPA2-Enterprise are interoperable.
Data Encryption	Click to open the following data encryption types: • None: No encryption. • WEP: WEP encryption provides two levels of security that use a 64-bit key (sometimes referred to as 40-bit) or a 128-bit key (also known as 104-bit). If you use encryption, all wireless devices on your wireless network must use the same encryption keys. • CKIP: Cisco Key Integrity Protocol is a Cisco proprietary security protocol for encryption in 802.11 media. CKIP uses Key Permutation (KP) and Message Sequence Number to improve 802.11 security in infrastructure mode. • TKIP: Provides per-packet key mixing, a message integrity check and a rekeying mechanism. • AES-CCMP: (Advanced Encryption Standard - Counter CBC-MAC Protocol) Used as the data encryption method whenever strong data protection is important.

Enable 802.1X (Authentication Type)	Click to open the following 802.1X authentication types: - TLS - TTLS - PEAP - LEAP - EAP-FAST - EAP-SIM: If in administrator mode, this only available for Pre-logon/Common profiles, not Persistent. - EAP-AKA: If in administrator mode, this only available for Pre-logo/Common profiles, not Persistent. Certain Authentication Types require that you obtain and install a client certificate. See Set up a Client with TLS authentication or consult your administrator.
Authentication Protocols	Authentication Protocols apply only when Network Authentication is set to WPA-Enterprise or WPA2-Enterprise and Authentication Type is set to TTLS or PEAP. - PAP - CHAP - MS-CHAP - MS-CHAP-V2 - GTC - TLS
Cisco Options	Click to view the Cisco Compatible Extensions Options. **NOTE**: Cisco Compatible Extensions are automatically enabled for CKIP and LEAP profiles.
Advanced	Click to access the Advanced Settings and configure the following options listed. - Auto Connect: Select to automatically or manually connect to a profile. - Auto Import: Allows a network administrator to move this profile to other computers. (Visible on user profiles only.) - Band Selection: Select the band to use for this connection profile. - Mandatory Access Point: Select to associate the WiFi adapter with a specific access point.

	• Password Protection: Select to password protect a profile. • Start Application: Specify a program to be started when a wireless connection is made. • Maintain Connection: Select to remain connected to a user profile after log off. (Visible on user profiles only.) • User Name Format: Select the user name format for the authentication server. (Visible on administrator profiles only.) • PLC Domain Check: Select to verify the domain server's presence before the user login process is finished. (Visible on administrator profiles only.)
User Credentials	A profile configured for TTLS, PEAP, or EAP-FAST authentication requires one of the following log on authentication methods: • **Use Windows logon**: The 802.1X credentials match your Windows user name and password. Before connection, you are prompted for your Windows logon credentials. **NOTE**: For LEAP profiles, this option is listed as **Use Windows logon user name and password**. • **Prompt each time I connect**: Prompt for your user name and password every time you log onto the wireless network. **NOTE**: For LEAP profiles, this option is listed as **Prompt for the user name and password**. • **Use the following**: Use your saved credentials to log onto the network. ○ **User Name**: This user name must match the user name that is set in the authentication server by the administrator prior to client authentication. The user name is case-sensitive. This name specifies the identity supplied to the authenticator by the authentication protocol operating over the TLS tunnel. This identity is securely transmitted to the server only after an encrypted channel has been established. ○ **Domain**: Name of the domain on the authentication server. The server name identifies a domain or one of its sub-domains (for example,

	zeelans.com, where the server is blueberry. zeelans.com). - **Password**: Specifies the user password. The password characters appear as asterisks. This password must match the password that is set in the authentication server. - **Confirm Password**: Reenter the user password. - **Roaming Identity**: A Roaming Identity may be populated in this field or you can use %domain%\%username% as the default format for entering a roaming identity. When 802.1X Microsoft IAS RADIUS is used as an authentication server, the server authenticates the device using the **Roaming Identity** from Intel PROSet/Wireless WiFi software, and ignores the **Authentication Protocol MS-CHAP-V2** user name. Microsoft IAS RADIUS accepts only a valid user name (dotNet user) for the Roaming Identity. For all other authentication servers, the Roaming Identity is optional. Therefore, it is recommended to use the desired realm (for example, anonymous@myrealm) for the Roaming Identity rather than a true identity. **NOTE**: Contact your administrator to obtain the domain name. **NOTE**: For LEAP profiles, this option is listed as **Use the following user name and password**.
Server Options	Select one of the following credential retrieval methods: • **Validate Server Certificate**: Select to verify the server certificate. **Certificate Issuer**: The server certificate received during TLS message exchange must be issued by this certificate authority (CA). Trusted intermediate certificate authorities and root authorities whose certificates exist in the system store are available for selection. If **Any Trusted CA** is selected, any CA in the list is acceptable. Click **Any Trusted CA** as the default or select a certificate issuer from the list. • **Specify Server or Certificate Name**: Enter the server name. The server name or domain to which the server belongs, depends on which of the following options has been selected.

	Server name must match the specified entry exactly: When selected, the server name must match exactly the server name found on the certificate. The server name should include the complete domain name (for example, Servername.Domain name). **Domain name must end with the specified entry**: When selected, the server name identifies a domain, and the certificate must have a server name that belongs to this domain or to one of its subdomains (for example, zeelans.com, where the server is blueberry. zeelans.com). **NOTE**: These parameters should be obtained from the administrator.
Certificate Options	To obtain a certificate for TLS authentication, select one of the following: **Use my smart card**: Select if the certificate resides on a smart card. **Use the certificate issued to this computer**: Selects a certificate that resides in the machine store. **Use a user certificate on this computer**: Click **Select** to choose a certificate that resides on this computer. **NOTE**: The Intel(R) PROSet/Wireless WiFi Connection Utility supports machine certificates. However, they are not displayed in the certificate listings. **Notes about Certificates**: The specified identity should match the **Issued to** identity in the certificate and should be registered on the authentication server (for example, RADIUS server) that is used by the authenticator. Your certificate must be valid with respect to the authentication server. This requirement depends on the authentication server and generally means that the authentication server must know the issuer of your certificate as a Certificate Authority. Use the same user name you used to log in when the certificate was installed.
Back	View the prior page in the Profile Wizard.
Next	View the next page in the Profile Wizard. If more security information is required then the next step of the Security Settings is displayed.
OK	Closes the Profile Wizard and saves the profile.

Cancel	Closes the Profile Wizard and cancels any changes made.
Help?	Provides the help information for the current page.

Back to Top

Back to Contents

[Back to Contents](#)

Administrator Tool

The Administrator Tool is used by the person who has administrator privileges on this computer. This tool is used to configure Pre-logon/Common profiles, and Persistent Connection profiles. The Administrator Tool can be used by an Information Technology department to configure user settings and to create custom install packages to export to other systems.

The Administrator Tool is located on the Tools menu. The Administrator Tool must be selected during a Custom installation of the Intel(R) PROSet/Wireless WiFi Connection Utility or the feature is not displayed.

Administrator Packages for Windows XP*

An Administrator Package is a self-extracting executable file that generally contains the WiFi connection utility, administrative profiles, and other settings. You can copy or send an administrative package to clients on your network. When the executable runs, the contents are installed and configured on the destination computer. If a profile is part of the package, the profile governs how the destination computer connects to a specific wireless network.

NOTE: To create and export a package for a computer running on Microsoft Windows Vista*,

you need to create the package on a computer running Windows Vista. You cannot create a package for Windows Vista on a computer running Microsoft Windows XP*.

Create a New Package

1. At the Tools menu, click **Administrator Tool**.
2. Enter the Administrator Tool password.
3. **Open Administrator Package**: Click **Create a Windows XP package**, or **Open an existing package**.



Name	Description
Create a Windows XP package	Create a package that can be exported to a user's computer running Microsoft Windows XP* operating system. This package allows export of all 802.1X authentication EAP-type Pre-logon/Common and Persistent profiles.
Create a Windows Vista package	Not Available. To create and export a package for a computer running on Microsoft Windows Vista*, you need to create the package on a computer running Windows Vista. You cannot create a package for Windows Vista on a computer running Microsoft Windows XP*.

Open an existing package	Select to browse for and open an existing package.

4. Click **OK**.
5. Configure the following options to be included in the package:

Name	**Description**
Profiles	Click **Include Profiles in this package**. Profiles can be shared with other users.
Application Settings	Click **Include Application Settings in this package**. Specify application settings to be enabled.
Adapter Settings	Click **Include Adapter Settings in this package**. Specify initial values for adapter settings used on this computer.
EAP-FAST A-ID Groups	Click **Include A-ID Groups**. Add A-ID Group to support multiple PACs from multiple A-IDs.

6. Click **Close**.
7. You are notified: **The current package is changed. Would you like to save the changes?**
8. Click **Yes**. Save the executable file to a directory on the local disk drive.
9. Click **Save**. The file is created. This may take several minutes.
10. Click **Finished** to view the package contents.
    - Click **Apply this package to this computer** if you want to use the package configuration on the Administrator's computer.
    - Copy the executable file to any user's computer to install the configuration that has been saved in the package. When you execute the package file, it is a silent install.
11. Click **OK**.

NOTE: You can also select **Save Package** on the **File** menu to save the package.

Edit a Package

1. Access the Administrator Tool.
2. On the Open Administrator Package page, click **Open an existing package** to edit an existing package.
3. Click **Browse**. Locate the package's executable file.
4. Click **Open**. Make your updates to the package settings.
5. Click **Close**.
6. You are notified: **The current package is changed. Would you like to save the changes?**
7. Click **Yes**. Save the executable file to a directory on the local disk drive.

NOTE: You can also select **Open Package** on the **File** menu to edit an

Administrator Package.

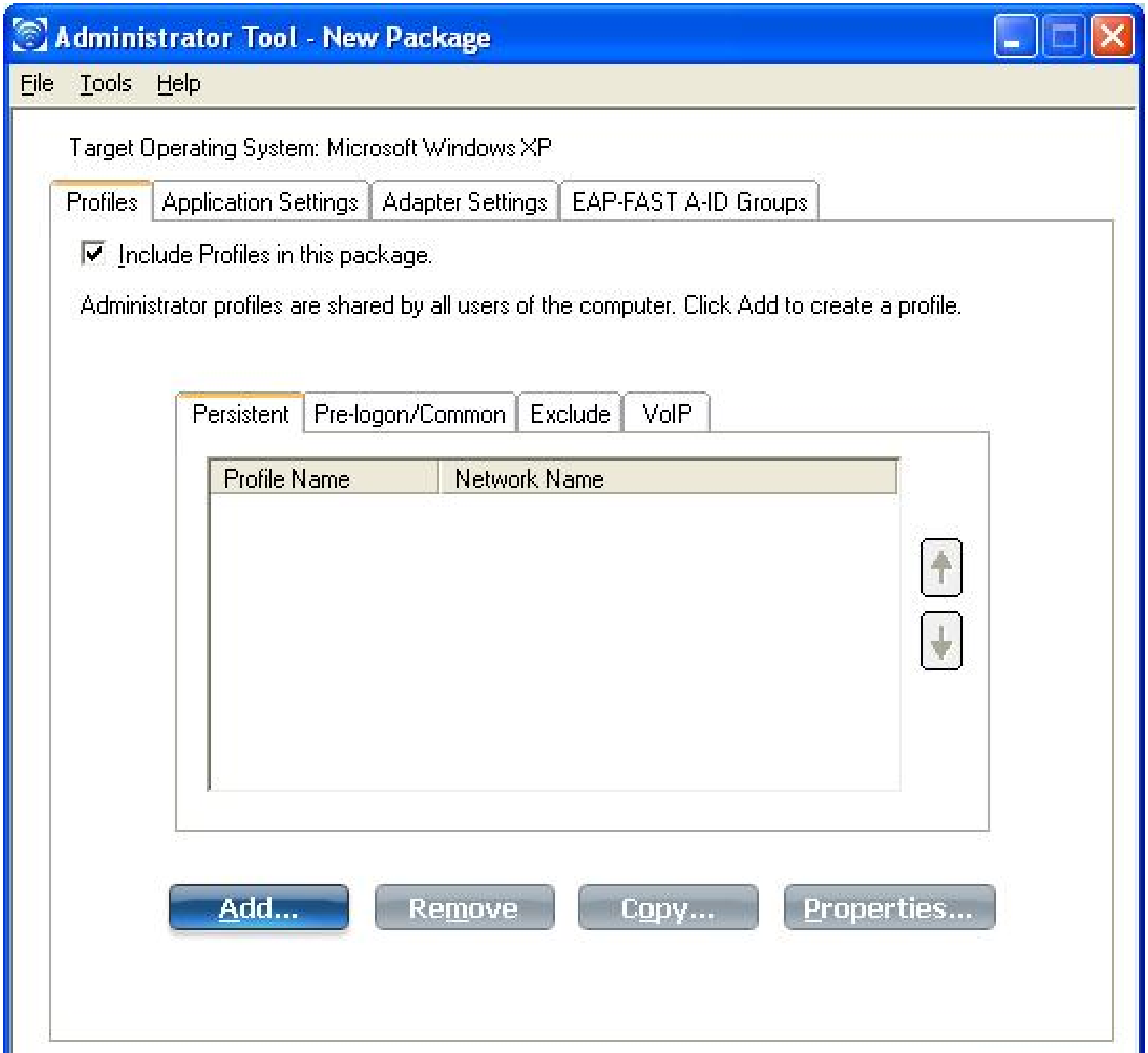
Administrator Profiles

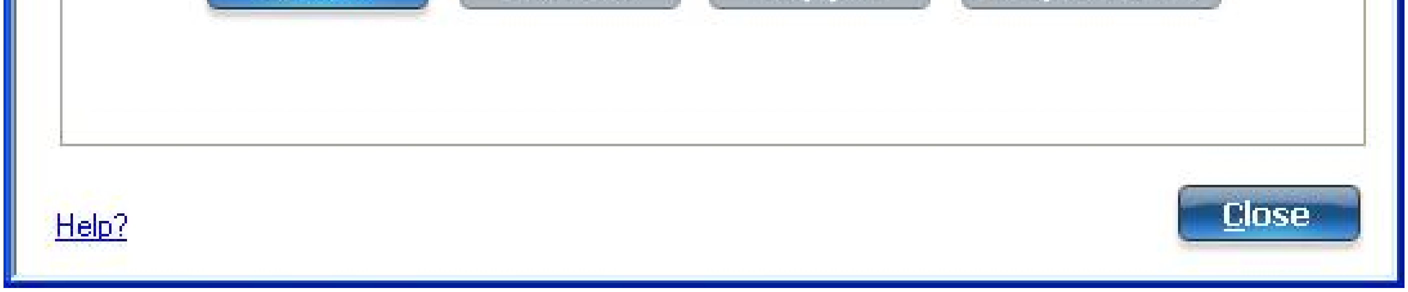
Administrator Profiles are managed by the network administrator. These profiles can be exported to other computers.

These profiles are common or shared by all users on this computer. However, end users cannot modify these profiles. They can only be modified from the Administrator Tool, which is password protected.

There are two types of Administrator Profiles: Persistent and Pre-logon/Common.

You can also configure Voice over IP (VoIP) settings for export to a soft-phone application.





Persistent Profiles

Persistent profiles are applied at boot time or whenever no one is logged on the computer. After a user logs off, a Persistent profile maintains a wireless connection either until the computer is turned off or a different user logs on.

Persistent profile key points:

- The following types of profiles can be created as Persistent profiles:
  - All profiles that do not require 802.1X authentication (for example, Open authentication with WEP encryption, Open authentication with no encryption).
  - All profiles with 802.1X authentication that have the credentials saved: LEAP or EAP-FAST.
  - Profiles with security settings that include the "Use the following user name and password" option.
  - Profiles that use the machine certificate to authenticate.
  - WPA*-Enterprise profiles that do not use a user certificate.
  - WPA-Personal profiles.
- Persistent profiles are applied at system power up and after a user logs off.

  NOTE: The WiFi connection utility supports machine certificates. However, they are not displayed in the certificate listings.

To create a Persistent profile:

1. Click **Include Profiles in this package**.
2. Click **Persistent**.
3. Click **Add** to open the General Settings.
4. **Profile Name**: Enter a descriptive profile name.
5. **WiFi Network Name (SSID)**: Enter the name of your WiFi network.
6. **Operating Mode: Network (Infrastructure)** is selected by default.
7. **Administrator Profile Type**: **Persistent: Active when no users are logged on** is selected.
8. Click **Next**.
9. Click **Enterprise Security** to open the **Security Settings**. See TLS, TTLS, PEAP, LEAP, or EAP-FAST for 802.1X security configuration information.
10. Click **OK**.

Pre-logon/Common

Pre-logon/Common profiles are applied prior to a user log on. If Single Sign On support is installed, the connection is made prior to the Windows log-on sequence (Pre-logon/Common).

If Single Sign On support is not installed, the profile is applied once the user session is active. Pre-logon/Common profiles always appear at the top of the Profiles list. Users can still prioritize profiles that they have created but they cannot reprioritize Pre-logon/Common profiles. Because these profiles appear at the top of the Profiles list, the WiFi connection utility automatically attempts to connect to the Administrator profiles first before any user-created profiles.

> **NOTE**: Only administrators can create or export Pre-logon/Common profiles.

Pre-logon Connect key points are:

- Pre-logon Connect is active only at the Windows log on.
- The following types of profiles can be created as Pre-logon/Common profiles:
  - 802.1X PEAP, TTLS or EAP-FAST profiles that use either the "Use Windows Logon user name and password" or "Use the following user name and password" credentials when configuring the profile's security settings.
  - LEAP profiles that use the "Prompt for the user name and password." credentials when configuring the profile's security settings.
  - 802.1X PEAP or TTLS profiles with user or machine certificates (the user must have administrative rights to use machine certificates).
  - TLS profiles that use digital certificates to verify the identity of a client and a server.
  - EAP-SIM profiles that use a Subscriber Identity Module (SIM) card to validate your credentials with the network.
  - All non-802.1X (Open and WEP) Common or User Based profiles.
- A Pre-logon/Common profile is applied at Windows user log-on time.

Pre-logon/Common Connection Status

Pre-logon/Common profiles support is installed during a **Custom** install of the WiFi connection utility. See Install or Uninstall the Single Sign On Feature for more information.

> **NOTE**: If the Single Sign On or Pre-logon Connect features are not installed, an administrator is still able to create Pre-logon/Common profiles for export to a user's computer.

The following describes how the Pre-logon Connect feature functions from system power-up. The assumption is that a saved profile exists. This saved profile has valid security settings marked with "Use Windows Logon user name and password" that are applied at the time of Windows log on.

1. After a system power-up, enter your Windows log on domain, user name, and password.
2. Click **OK**. The Pre-logon/Common profile status page displays the progress of the network connection. After the WiFi adapter is connected to the network access point, the Status page closes and the Windows user logs on.
   - If the corresponding access point rejects your credentials during the Pre-logon/

Common connection, you will be prompted for your user credentials.
- Enter your credentials.
- Click **OK**. The profile is applied and the Status page displays the progress of the connection status until you are logged onto Windows.
- Click **Cancel** on the Credentials page to select another profile.

NOTE: A user certificate can only be accessed by a user that has been authenticated on the computer. Therefore, a user should log onto the computer once (using either a wired connection, alternate profile or local log in) before using a Pre-logon/Common profile that authenticates with a user certificate.

When you log off, any wireless connection is disconnected and a persistent profile (if one is available) is applied. Under certain circumstances, it is desirable to maintain the current connection (for example, if user-specific data needs to be uploaded to the server post-log off or when roaming profiles are used).

Create a profile that is marked as both Pre-logon/Common and persistent to achieve this functionality. If such a profile is active when the user logs off, the connection is maintained.

To create a Pre-logon/Common Profile:

1. Click **Include Profiles in this package**.
2. Click **Pre-logon/Common**.
3. Click **Add** to open the General Settings.
4. **Profile Name**: Enter a descriptive profile name.
5. **WiFi Network Name (SSID)**: Enter the network identifier.
6. **Operating Mode: Network (Infrastructure)** is selected by default.
7. **Administrator Profile Type**: **Pre-logon/Common: Active when a user is logged on. This profile is shared by all users**. This profile type is already selected.
8. Click **Next**.
9. Click **Advanced** to open and configure the Advanced Settings. See Advanced Settings.
10. Click **OK** to close the Advanced Settings.
11. Click **Enterprise Security** to open the **Security Settings**. See EAP-SIM, TLS, TTLS, PEAP, LEAP, or EAP-FAST for 802.1X security configuration information.
12. Click **OK** to save the profile and add it to the Administrator profiles list.

NOTE: If a Persistent connection was already established, a Pre-logon/Common profile is ignored unless the profile is configured with both Pre-logon/Common and Persistent connection options.

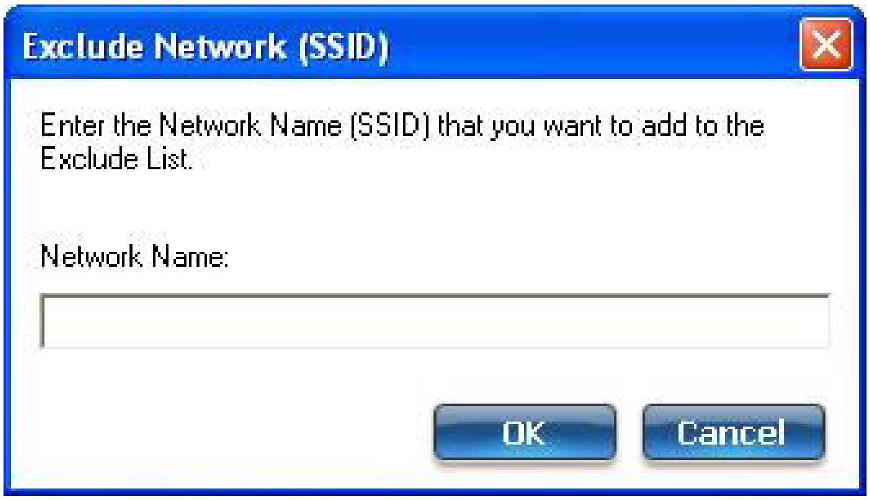
Exclude Networks

Administrators can designate networks to be excluded from connection. Once a network is excluded, only an administrator can remove the network from the Exclude list. The excluded

network is displayed in the Exclude List Management and is indicated by this icon: 

To exclude a network:

1. Click **Include Profiles in this package**.
2. Click **Exclude**.
3. Click **Add** to open the Exclude Network (SSID).
4. **Network Name**: Enter the network name of the network that you want to exclude.
5. Click **OK** to add the network name to the list.



To remove a network from exclusion:

1. Select the network name in the Exclude list.
2. Click **Remove**. The network is deleted from the list.

Voice over IP (VoIP) Connection

The WiFi connection utility supports VoIP third-party soft-phone applications. Third-party VoIP applications support voice codecs. Codecs generally provide a compression capability to save network bandwidth. The WiFi connection utility supports the following International Telecommunications Union (ITU) codec standards:

Codec	**Algorithm**
ITU G.711	PCM (Pulse Code Modulation)
ITU G.722	SBADPCM (Sub-Band Adaptive Differential Pulse Code Modulation)

ITU G.723	Multi-rate Coder
ITU G.726	ADPCM (Adaptive Differential Pulse Code Modulation)
ITU G.727	Variable-Rate ADPCM
ITU G.728	LD-CELP (Low-Delay Code Excited Linear Prediction)
ITU G.729	CS-ACELP (Conjugate Structure Algebraic-Code Excited Linear Prediction)

An administrator can export VoIP settings to configure various codec data rates and frame rates to improve voice quality in VoIP transmissions.

To configure VoIP settings:

> **NOTE**: Ensure Voice over IP is not disabled in the Administrator Tool Application Settings. It is enabled by default.

1. Click **Include Profiles in this package**.
2. Click **VoIP**.
3. Click **Add** to open the **Create VoIP Profiles** page.
4. Select the Codec bandwidth, application usage, and frame rate. For Voice Data:

   G711 has 10ms frame rate with 64kbps bit rate
   G722 has 10ms frame rate with 64kbps bit rate
   G723 has 30ms frame rate with either 5.3kbps or 6.4kbps bit rate
   G726-32 has 10ms frame rate with 32kbps bit rate
   G728 has 2.5ms frame rate with 16kbps bit rate
   G729 has 10ms frame rate with 10kbps bit rate

   Select parameters from the drop down menus.

Codec	Usage	Frame Rate

• G711_64kbps • G722_64kbps • G722_56kbps • G722_48kbps • G722_1_32kbps • G722_1_24kbps • G722_1_16kbps • G726_16kbps • G726_24kbps • G726_32kbps • G726_40kbps • G728_16kbps • G729a_8kbps • G729e_11_8kbps • GIPS_iPCM_VARIABLE • G722_2_VARIABLE	• Interactive Voice • Audio Conference • Voice Data • Video • Streaming Audio	• 20 • 30

5. Click **OK** to return to the Profiles list.
6. Click **Close** to save the profile settings to a package.

EAP-FAST A-ID Groups

> **NOTE**: This feature is unavailable if **CCXv4** is not selected in the Administrator Tool Application Settings

An Authority Identifier (A-ID) is the RADIUS server that provisions Protected Access Credential (PACs) A-ID groups. A-ID groups are shared by all users of the computer and allow EAP-FAST profiles to support multiple PACs from multiple A-IDs.

The A-ID groups can be pre-configured by the administrator and set up through an Administrator Package on a user's computer. When a wireless network profile encounters a server with an A-ID within the same group of the A-ID specified in the wireless network profile, it uses this PAC without a prompt to the user.

To add an A-ID Group:

1. Select **Include A-ID Groups**.
2. Click **Add**.
3. Enter a new A-ID group name.
4. Click **OK**. The A-ID group is added to the A-ID Group list.

If the A-ID group is locked, then additional A-IDs cannot be added to the group.

To add an A-ID to an A-ID group:

1. Select a group from the A-ID Groups list.
2. Click **Add** in the A-IDs section.
3. Select an A-ID.
4. Click **OK**. The A-ID is added to the list.

Once an A-ID group has been selected, the A-IDs are extracted from the PACs on the A-ID group server. The list of A-IDs is automatically populated.

Administrator Tasks

How to Obtain a Client Certificate

If you do not have any certificates for EAP-TLS (TLS) or EAP-TTLS (TTLS) you must obtain a client certificate to allow authentication.

Certificates are managed from either Internet Explorer or the Microsoft Windows Control Panel.

Windows XP: When a client certificate is obtained, do not enable strong private key protection. If you enable strong private key protection for a certificate, you need to enter an access password for the certificate every time this certificate is used. You must disable strong private key protection for the certificate if you configure the service for TLS or TTLS authentication. Otherwise, the 802.1X service fails authentication because there is no logged in user to provide the required password.

Notes about Smart Cards

After a Smart Card is installed, the certificate is automatically installed on your computer and is chosen from the personal certificate store and root certificate store.

Set up a Client with TLS Network Authentication

Step 1: Obtain a certificate

To allow TLS authentication, you need a valid client certificate in the local repository for the logged-in user's account. You also need a trusted CA certificate in the root store.

The following information provides two methods for obtaining a certificate:

- From a corporate certification authority (CA) implemented on a Windows 2000 server.
- Import a certificate from a file with Internet Explorer's certificate import wizard.

If you do not know how to obtain a user certificate from the CA, consult your administrator for the procedure.

To install the CA on the local machine:

1. Obtain the CA and store it on your local drive.
2. Click **Import**. The Certificate Import Wizard opens.
3. Click **Next**.
4. Click **Browse** to locate the certificate on your local drive.
5. Click the exported certificate.
6. Click **Open**.
7. Click **Next**.
8. Click **Place all certificates in the following store**.
9. Click **Browse** to open the **Select Certificate Store**.
10. Click **Show physical stores**.
11. Click **OK**.
12. From the list of stores, scroll up and expand **Trusted Root Certificate Authorities**.
13. Click **Local Computer.**
14. Click **OK**.
15. Click **Next**.
16. Click **Finish** to complete the process.
17. Reboot after a certificate is installed.

Use Microsoft Management Console (MMC) to verify that the CA is installed in the machine store.

1. In the Start menu, click **Run**.
2. Enter **MMC**.
3. Click **OK** to open The Microsoft Management Console.
4. Click **File**.
5. Click **Add/Remove Snap-in**.
6. Click **Add** to open the Add Standalone Snap-in page.
7. Click **Certificates**.
8. Click **Add**.
9. Click **Computer account**.
10. Click **Next**.
11. Click **Finish**.
12. Click **Close**.
13. Click **OK**.
14. In the console, click **Certificates (Local Computer)**.
15. Click **Trusted Root Certificate Authorities**.
16. Click **Certificates**.
17. Verify that the CA you just installed is listed.
18. Click **File**.
19. Click **Exit** to close the console.

Obtain a certificate from a Microsoft Windows 2000* CA:

1. Start Internet Explorer and browse to the Certificate Authority HTTP Service (use an URL, for example, http://yourdomainserver.yourdomain/certsrv with certsrv being the

command that brings you to the certificate authority. You can also use the IP address of the server machine. For example, "192.0.2.12/certsrv."

2. Logon to the CA with the name and password of the user account you created on the authentication server. The name and password do not have to be the same as the Windows log on name and password of the current user.
3. On the Welcome page of the CA, select **Request a certificate task and submit the form**.
4. **Choose Request Type**: Select **Advanced request**.
5. Click **Next**.
6. **Advanced Certificate Requests**: Select **Submit a certificate request to this CA using a form**.
7. Click **Submit**.
8. **Advanced Certificate Request**: Select **User certificate template**.
9. Click **Mark keys as exportable**.
10. Click **Next**. Use the provided defaults.
11. **Certificate Issued**: Click **Install this certificate**.

    NOTE: If this is the first certificate you have obtained, the CA first asks you if it should install a trusted CA certificate in the root store. This is not a trusted CA certificate. The name on the certificate is that of the host of the CA. Click **Yes**. You need this certificate for both TLS and TTLS.

12. If your certificate was successfully installed, you see the message, "Your new certificate has been successfully installed."
13. To verify the installation, click **Internet Explorer > Tools > Internet Options > Content > Certificates**. The new certificate should be installed in the Personal folder.

Import a Certificate from a File

1. Open Internet Properties (right-click on the Internet Explorer icon on the desktop.
2. Select **Properties**.
3. **Content**: Click **Certificates**. The list of installed certificates appears.
4. Click **Import** to open the Certificate Import Wizard.
5. Select the file.
6. Specify your access password for the file. Clear **Enable strong private key protection**.
7. **Certificate store**: Click **Automatically select certificate store based on the type of certificate** (the certificate must be in the user accounts personal store to be accessible).
8. Proceed to **Completing the Certificate Import** and click **Finish**.

To configure a profile with WPA authentication with WEP or TKIP encryption that uses TLS authentication:

> **NOTE**: Obtain and install a client certificate, See Step 1 or consult your administrator.

Specify the certificate used by the WiFi connection utility.

1. On the Profile page, click **Add** to open General Settings.

2. **Profile Name**: Enter a profile name.
3. **WiFi Network Name (SSID)**: Enter the network identifier.
4. **Operating Mode: Network (Infrastructure)** is selected by default.
5. Click **Next** to open the **Security Settings**.
6. Click **Enterprise Security**.
7. **Network Authentication**: Select **Open** (Recommended).
8. **Data Encryption**: Select **WEP**.
9. **802.1X Enabled**: Selected.
10. **Authentication Type**: Select **TLS**.

Step 1 of 2: TLS User

1. Obtain and install a client certificate.
2. Select one of the following to obtain a certificate:

Name	**Description**
Static Password	On connection, enter the user credentials.
One-time password (OTP)	Obtain the password from a hardware token device.
PIN (Soft Token)	Obtain the password from a soft token program.

3. Click **Next**.

Step 2 of 2: TLS Server

1. Select one of the following credential retrieval methods: Validate Server Certificate or Specify Server or Certificate Name.
2. Click **OK**. The profile is added to the Profiles list.
3. Click the new profile at the end of the Profiles list. Use the up and down arrows to change the priority of the new profile.
4. Click **Connect** to connect to the selected WiFi network.
5. Click **OK** to close the application.

Back to Top

Back to Contents

Back to Contents

Set Administrator Password

A user cannot modify Administrator settings or profiles unless they have the password for this tool. When you first access the Administrator Tool, you are required to enter a password. The password must not exceed 100 characters (although the field will only display up to 56 characters). Null passwords are not allowed.

1. **Password**: Create a password (maximum 100 characters).
2. **Confirm Password**: Reenter the password.
3. Click **OK**. The Open Administrator Package displays.

To change or unlock the existing password:

1. On the Tools menu, click **Administrator Tool**.
2. Click **Change Password** on the password entry form.
3. **Old Password**: Enter the existing password.
4. **New Password**: Enter the new password.
5. **Confirm Password**: Reenter the new password again.
6. Click **OK** to save the new password and enter the Administrator Tool.

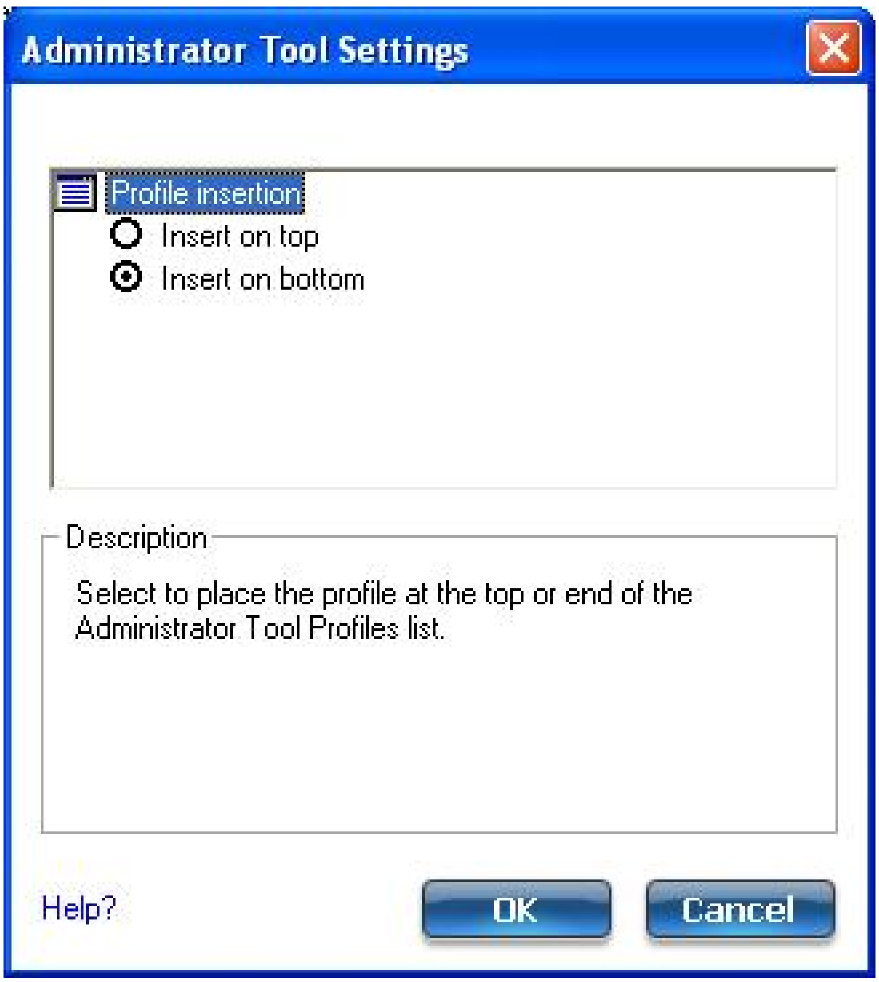
Back to Top

Back to Contents

Back to Contents

Administrator Tool Settings

These settings allow the administrator to control where profiles are placed in the Administrator's Profiles list.



Name	Description	
Profile Insertion: Select one of the following to place Administrator profiles within a Administrator's Profiles list.	**Insert on top**	Select to place Administrator profiles at the top of the Administrator's Profiles list (Persistent, Pre-logon/Common or Voice over IP profiles)

	Insert on bottom	Select to place Administrator profiles at the end of the Administrator's Profiles list. (Persistent, Pre-logon/Common or Voice over IP profiles)
OK	Save settings and close the page.	
Cancel	Cancel settings and close the page.	
Help?	Provides help information for this page.	

How to Use

1. Open the Administrator Tool.
2. Click **Tools > Settings** to open the **Administrator Tool Settings**.
    - Select **Insert on top** to always place Administrator profiles at the top of the Administrator Tool's Profiles list.
    - Select **Insert on bottom** to always place Administrator profiles at the bottom the Administrator Tool's Profiles list.
3. Click **OK** to close and return to the Administrator Tool.

Back to Top

Back to Contents

Back to Contents

Application Settings (Administrator Tool)

An administrator can configure the Intel(R) PROSet/Wireless WiFi Connection Utility settings to control how the application behaves on the user's computer, and to select what level of control users have over various aspects of their wireless connections. These settings are configured using the Administrator Tool, and are not the same as those listed under the Tools Menu.

To configure Application Settings:

1. Click **Include Application Settings in this package**.
2. Select the settings that you want. Some settings require more information. Each setting is listed in the next table.

Name	Description
802.1X Authentication	Enable a user to create or connect to profiles that support different 802.1X authentication EAP types. Select which 802.1X authentication EAP types you want enabled on a user's computer: EAP LEAP, EAP PEAP, EAP TLS, EAP SIM, EAP TTLS, EAP FAST, EAP AKA.
AAA In Control	Notify when another application uses the WiFi adapter.
Adapter Switching	If enabled, then whenever a valid wired Ethernet connection is detected, the WiFi connection utility will automatically close any wireless network connections and turn off the wireless radio. If the system looses its wired Ethernet connection, the WiFi connection utility will automatically turn on the WiFi adapter radio and attempt to connect to the last connected profile. If the last connected network is not available, the WiFi connection utility will attempt to connect to the first available wireless network based on the preferred Profile List. **NOTE**: This behavior is for the system as a whole and is not specific to any user.

	NOTE: If the user has manually turned off the wireless radio, the radio will not turn on again when an wired Ethernet connection is lost. The user must turn the radio back on for wireless connections to be established.
Administrator Tool	Disable access to the Administrator Tool on a user's computer.
Application Auto Launch	Enabling this feature lets the user specify an application that will start up whenever a particular network profile connects. The user selects the profile and can then specify an application, batch file, or script. For example, the user may want a Virtual Private Network (VPN) session to start automatically whenever the laptop connects to a specific wireless network. If this feature is unchecked (disabled), then the user cannot specify any application to startup automatically when a given network profile connects.
Application On Radio Toggle	Enables a third-party application to disable the Intel (R) PROSet/Wireless WiFi Connection Utility, **WiFi On / WiFi Off** button.
CCXv4	Select **Enable CCXv4** to Enable Cisco Compatible Extensions, version 4 (CCXv4) features for EAP-FAST profiles. **NOTE**: The EAP-FAST Authority Identifier (A-ID) Groups feature in the Administrator Tool is unavailable if CCXv4 is not enabled. Select which of the following prompts to enable or disable on a user's computer for EAP-FAST PAC provisioning: **Turn off prompts and warnings for unauthenticated provisioning**: Option to turn off prompts and warnings for PAC auto-provisioning if there is no PAC or there is no PAC that matches the A-ID sent by the server that it is connected to. **Turn off prompts when switching default server (A-ID)**: Option to turn off prompts when a client encounters a server that has provisioned a PAC before but is not currently selected as the default server.

	Turn off unauthenticated provisioning after PAC is provisioned: Option to turn off auto-provisioning automatically after a PAC for that A-ID has been provisioned. **NOTE**: This feature is installed through an Administrator Package when a user's computer has one of the following adapters: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN • Intel(R) Wireless WiFi Link 4965AG_ • Intel(R) PRO/Wireless 3945ABG Network Connection
Cache Credentials	Select to save credentials after a user logs on. If the wireless connection temporarily disconnects, the saved credentials are used upon reconnection. The credentials are cleared when the user logs off. **NOTE**: if cleared, the **Prompt each time I connect** option is unavailable when creating profiles.
Certificate Expiry Warning	If specified, the WiFi connection utility will warn users when the certificates are going to expire. The provided URL will allow them to update their certificates from a certificate server.
Device to Device (ad hoc)	Enable or disable whether a user is able to either create Device to Device (ad hoc) profiles or join Device to Device (ad hoc) networks. Select one of the following to enable or disable whether the user can connect to device to device networks: • Enable device to device networking • Enable only secure device to device networking • Disable device to device networking Select to either allow a user to configure profiles with device to device (ad hoc) settings or prevent

	configuration of Device to Device (ad hoc) profiles. • Show device to device application settings • Hide device to device application settings To remove the Device to Device (ad hoc) operating mode from the Create WiFi Profile General Settings, select both **Disable device to device networking** and **Hide device to device application settings**. This prevents a user from creating profiles that support Device to Device (ad hoc) network.
Import and Export	Select to import to or export profiles from a user's computer. Enable permits auto import of user profiles when copied to an auto import folder.
Maintain Connection	Select to hide the Maintain Connection option in the Create WiFi Profile Advanced Settings. This Maintain Connection option maintains the wireless connection with a user profile after log off. **NOTE**: The Maintain Connection option may be used with Nortel VPN client when it is configured to **Logoff on Connect**.
Maintain SmartCard Connection	Select to maintain the connection if the smart card is removed while the wireless device is connected to a network that uses smart card credentials. The default behavior for the WiFi connection utility is to close the connection that uses smart card credentials if the smart card is removed. Turning this feature On will cause the connection to remain connected (unless re-authentication is required for another reason). Select to maintain a connection if the smart card is removed while the wireless device is connected to a network using smart card/SIM credentials. **NOTE**: This setting is not available for Windows Vista* client profiles.
Message On Radio Toggle	Enables a third-party application to notify a user that the Intel(R) PROSet/Wireless WiFi Connection Utility **WiFi On / Off** switch is disabled.

Microsoft Windows XP Coexistence	Select **Enable Microsoft Wireless Zero Configuration and Intel PROSet/Wireless WiFi to coexist on this system**. Enable this option to allow Microsoft Wireless Zero Configuration and the WiFi connection utility to exist together on this system. When you select this option, you prevent Microsoft Windows XP Wireless Zero Configuration Service from being disabled when the WiFi connection utility is enabled.
Persistent Connection	Select **Ensure that persistent connection and computer policies are updated prior to user log on**. **NOTE**: Updating policies may delay the log on screen for up to two minutes.
Pre-logon Cisco Mode	Enable Cisco Mode during a Pre-logon connection. Cisco access points have the capability to support multiple WiFi network names (SSIDs) but only broadcast one. In order to connect to such an access point, an attempt is made to connect with each profile. This is referred to as Cisco Mode. **NOTE**: The Pre-logon connection may increase the connection time.
Profile Connectivity	Control profile connection by the user. **Disable user-profile switching**. Leaving this setting Off lets the user connect to both user and administrator profiles. By turning this setting On, the user can only connect to administrator profiles. The administrator also chooses which administrator profiles are available to the user, as follows: • Allow the user to connect to All administrator profiles. • Allow the user to only connect to the First administrator profile.

Security Level	Select the security level on a user's computer. **Users are able to connect to profiles only with this security level**. • Allow the user to connect to networks with Personal Security only.
Shared Folder Notification	Select the shared folder notification setting on a user's computer. • Unshare shared folders automatically when connected to an unsecured network. • Disable this notification. • Notify when connected to an unsecured network (default).
Single Sign On	Select which Administrator Profile types are enabled on a user computer. • **Persistent Connection** : Profiles are active during start up and when no user is logged onto the computer. • **Pre-logon or Common Connection**: Profiles are active immediately once a user logs onto the computer. Common profiles are enabled if Pre-logon or Common features are not installed on a user's computer. Common profiles are active after a user has logged on and the session becomes active. Persistent and Pre-logon or Common profiles are placed at the top of the user's profiles list. They cannot be changed or deleted by a user.

Support Information	Specify the support information displayed in the **About** box of the WiFi connection utility. • **Support URL**: Enter the support center web site that you want your customers to access for technical support. • **Support Phone Number**: Enter the telephone number that you want your customers to call for technical support.
Voice over IP	Enables third-party software to use the VoIP application on a user's computer. The default setting enables this feature. **NOTE**: This feature is installed through an Administrator Package when a user's computer has one of the following adapters: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN • Intel(R) Wireless WiFi Link 4965AG_ • Intel(R) PRO/Wireless 3945ABG Network Connection
Wi-Fi Manager	Select which Wi-Fi manager controls a user's wireless connections. Use either the previous logged on user's Wi-Fi manager or allow each user to select their preferred Wi-Fi manager. • Allow all users to switch between the WiFi connection utility and Microsoft Windows XP Wireless Zero Configuration after log on. • The Wi-Fi manager at log on is determined by the active Wi-Fi manager when the last user logged off.

Wi-Fi Protected Setup*	The WiFi connection utility can be configured to operate as a registrar for a Wi-Fi Protected Setup supported access points. The registrar securely transfers the access point key or password automatically or manually with a USB flash drive or other external device. • Enable registering other devices (default). • Hide Enable Device Registration application setting. Select to enable the WiFi connection utility to register other devices. Also select to hide the Enable Device Registration setting in the WiFi connection utility application settings to block user to change the settings. **NOTE**: This feature is installed through an Administrator Package when a user's computer has one of the following adapters: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN • Intel(R) Wireless WiFi Link 4965AG_ • Intel(R) PRO/Wireless 3945ABG Network Connection
WiFi On/Off	Control the wireless radio. • **No change**: The radio is not turned on or off. • **Turn WiFi Off**: The profile turns the radio off. • **Turn WiFi On**: The profile turns the radio on. • **Turn off 802.11a radio only**: This becomes selectable if **Turn WiFi On is** enabled. • **Disable WiFi On/Off selection**: Select to prevent a user from accessing the **WiFi On/Off** control on the WiFi connection utility main window or Taskbar menu. A user is notified that **The feature is disabled by the administrator** if they attempt to turn on or off the radio control. • **Add 802.11a Radio On/Off selection**:

	Select to allow the user to turn on/off the 802.11a radio separately from the 802.11b/g radio. If you select this, the **Disable 802.11a Radio On/Off selection** becomes available. Select this to show the 802.11a radio On/Off control, but disable it. This lets you give the user individual control over the radios. Once this feature is installed on a user's computer, follow the instructions below to turn on or off the 802.11a radio control. To turn off the 802.11a radio: 1. On the WiFi connection utility main window, click the **WiFi On** button. The list of radio options is displayed. 2. Select **802.11a Radio Off**. The 802.11a radio is now inactive. To turn on the 802.11a radio: 1. On the WiFi connection utility main window, click the **802.11a Radio Off** button. The list of radio options is displayed. 2. Select **WiFi On**. The 802.11a radio is now active. **NOTE**: The option **Add 802.11a Radio On/Off selection** is available only for WiFi adapters that support 802.11a, 802.11b and 802.11g. This feature is not installed through an Administrator Package when a user's computer has an Intel(R) PRO/ Wireless 2200BG Network Connection.
Close	Closes the Administrator Tool.
Help?	Provides help information for this page.

Back to Contents

Adapter Settings (Administrator)

The Adapter Settings screen controls and displays the device properties for the WiFi adapter installed on a computer. The WiFi adapter may be any one of the following:

- Intel(R) WiMAX/WiFi Link 5350
- Intel(R) WiMAX/WiFi Link 5150
- Intel(R) WiFi Link 5300
- Intel(R) WiFi Link 5100
- Intel(R) Wireless WiFi Link 4965AGN
- Intel(R) Wireless WiFi Link 4965AG_
- Intel(R) PRO/Wireless 3945ABG Network Connection
- Intel(R) PRO/Wireless 2915ABG Network Connection
- Intel(R) PRO/Wireless 2200BG Network Connection.

To configure Adapter Settings:

1. From within the Administrator tool, click **Include Adapter Settings in this package**.
2. For each setting listed in the table below, select one of the following options:
   - **Use default value**: Resets the setting on the user machine to the default value.
   - **No change**: (For Windows XP* users only.) Maintains the user selected value. The administrator decides not to enforce all the settings on a user's computer. The user can change the WiFi adapter setting values from the WiFi connection utility Advanced menu.
   - **No change**: (For Windows Vista* users only.) Maintains the user selected value. The administrator decides not to enforce all the settings on a user's computer. The user can change the WiFi adapter setting values at the Device Manager.
   - **Select the value**: The administrator selects the value that is to be used on the user's computer.

WiFi Adapter Settings Description

Following are descriptions of the WiFi adapter settings.

Name	Description

802.11n Channel Width (2.4 GHz)	Set high throughput channel width to maximize performance. Set the channel width to **Auto** or **20MHz**. **Auto** is the default setting. Use 20MHz if 802.11n channels are restricted. **NOTE**: This setting is available only if the WiFi adapter is one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100
802.11n Channel Width (5.2 GHz)	Set high throughput channel width to maximize performance. Set the channel width to **Auto** or **20MHz**. **Auto** is the default setting. Use 20MHz if 802.11n channels are restricted. **NOTE**: This setting is available only if the WiFi adapter is one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN
802.11n Mode	The 802.11n standard builds upon previous 802.11 standards by adding multiple-input multiple-output (MIMO). MIMO increases data throughput to improve transfer rate. Select **Enabled** or **Disabled** to set the 802.11n mode of the WiFi adapter. Enabled is the default setting. **NOTE**: This setting is available only if the WiFi adapter is one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN **NOTE**: To achieve transfer rates greater than 54 Mbps on 802.11n connections, WPA2*-AES security

	must be selected. No security (**None**) can be selected to enable network setup and troubleshooting. An administrator can enable or disable support for high throughput mode to reduce power-consumption or conflicts with other bands or compatibility issues.
Ad Hoc Channel	Unless the other computers in the ad hoc network use a different channel from the default channel, there is no need to change the channel. **Value**: Select the allowed operating channel from the list. • **802.11b/g**: Select this option when 802.11b and 802.11g (2.4 GHz) ad hoc band frequency is used. For this band, the default channel is 11. • **802.11a**: Select this option when 802.11a (5 GHz) ad hoc band frequency is used. For this band, the default channel is 36. **NOTE**: When an 802.11a channel is not displayed, initiating ad hoc networks is not supported for 802.11a channels.
Ad Hoc Power Management	Set power saving features for Device to Device (ad hoc) networks. • **Disable**: Select when connecting to ad hoc networks that contain stations that do not support ad hoc power management. • **Maximum Power Savings**: Select to optimize battery life. • **Noisy Environment**: Select to optimize performance or connecting with multiple clients. **NOTE**: This feature is only installed through an Administrator Package when a user's computer has one of the following WiFi adapters: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN • Intel(R) PRO/Wireless 3945ABG

Ad Hoc QoS Mode	Quality of Service (QoS) control in ad hoc networks. QoS provides prioritization of traffic from the access point over a wireless network based on traffic classification. WMM* (Wi-Fi Multimedia*) is the QoS certification of the Wi-Fi Alliance* (WFA). When WMM* is enabled, the WiFi adapter uses WMM to support priority tagging and queuing capabilities for Wi-Fi* networks. • **WMM Enabled** • **WMM Disabled** (default) **NOTE**: This feature is only installed through an Administrator Package when a user's computer has one of the following WiFi adapters: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN • Intel(R) PRO/Wireless 3945ABG
HD Mode	In a wireless network environment where several access points are nearby, this feature will reduce interference and improve your wireless connection. The default setting is for this to be turned off (disabled). **NOTE**: This setting is available only if the WiFi adapter is one of the following: • Intel(R) WiMAX/WiFi Link 5350 • Intel(R) WiMAX/WiFi Link 5150 • Intel(R) WiFi Link 5300 • Intel(R) WiFi Link 5100 • Intel(R) Wireless WiFi Link 4965AGN

Mixed Mode Protection	Use to avoid data collisions in a mixed 802.11b/11g/11a/11n environment. Request to Send/ Clear to Send (RTS/CTS) should be used in an environment where clients may not hear each other. CTS-to-self can be used to gain more throughput in an environment where clients are in close proximity and can hear each other. (CTS-to-self is not supported for 802.11n.)
Power Management (Administrator View)	When creating an administrator package, Power Management lets you select a balance between power consumption and WiFi adapter performance. **PSP** - Power Saving Mode **CAM** - Constantly Awake Mode Select one of the Power Saving Mode levels: **PSP CAM**: The client adapter is powered up continuously. **PSP Level 1**: PSP set at maximum power. **PSP Levels 2-4**: PSP set to maximize power. **PSP Level 5**: PSP set to maximize battery life. **PSP Auto**: Default in PSP Level 6: Balances between power consumption and battery life. **NOTE**: Power consumption savings vary based on infrastructure settings.
Preamble Mode	Changes the preamble length setting received by the access point during an initial connection. Always use **Auto Tx Preamble** to provide optimal network throughput. **Auto Tx Preamble** allows automatic preamble detection. If supported, short preamble should be used. If not, use **Long Tx Preamble**. **NOTE**: This setting is only available if the client WiFi adapter is an Intel(R) PRO/Wireless 2915ABG Network Connection or an Intel(R) PRO/Wireless 2200BG Network Connection.

Roaming Aggressiveness	This setting lets you define how aggressively a wireless client roams to improve connection to an access point. Click **Use default value** to balance between not roaming and performance or select a value from the list. **Values**: **0**: No Roaming: Your wireless client does not roam. Only significant link quality degradation causes it to roam to another access point. **1-3**: Allow Roaming **2**: Default: Balances between not roaming and performance. **4**: Maximum Roaming
Throughput Enhancement	Changes the value of the Packet Burst Control. • **Enable**: Select to enable throughput enhancement. • **Disable**: (Default) Select to disable throughput enhancement.
Transmit Power	If you decrease the transmit power, you reduce the WiFi radio coverage. **Default Setting**: Highest power setting **Values**: **Tx Minimum**: **Lowest Minimum Coverage**: Set the adapter to the lowest transmit power. Enables you to expand the number of coverage areas or confine a coverage area. Reduce the coverage area in high traffic areas to improve overall transmission quality and avoid congestion and interference with other devices. **Tx Level 1, Tx Level 2, Tx Level 3**: Set by country requirements. **Tx Maximum**: **Highest Maximum**

	Coverage: Set the adapter to the maximum transmit power level. Select for maximum performance and range in environments with limited additional radio devices. If you select **No change**, then this setting will not be changed at the user's computer. **NOTE**: The optimal setting is for a user to always set the transmit power at the lowest possible level still compatible with the quality of their communication. This allows the maximum number of wireless devices to operate in dense areas and reduce interference with other devices that this radio shares radio spectrum with. **NOTE**: This setting takes effect when either Network (Infrastructure) or Device to Device (ad hoc) mode is used.
Wireless Mode	Select which mode to use for connection to a wireless network: • **802.11a** only: Connect the wireless WiFi adapter to 802.11a networks only. • **802.11b** only: Connect the wireless WiFi adapter to 802.11b networks only. • **802.11g** only: Connect the wireless WiFi adapter to 802.11g networks only. • **802.11a and 802.11g**: Connect the wireless WiFi adapter to 802.11a and 802.11g networks only. • **802.11b and 802.11g**: Connect the wireless WiFi adapter to 802.11b and 802.11g networks only. • **802.11a, 802.11b, and 802.11g**: (Default) - Connect to either 802.11a, 802.11b or 802.11g wireless networks. **NOTE**: These wireless modes (Modulation types) determine the discovered access points displayed in the WiFi Networks list.

Back to Top

Back to Contents

Trademarks and Disclaimers

Back to Contents

Advanced Statistics (Advanced menu)

The Advanced Statistics provides current adapter connection information. This information defines how the adapter communicates with an access point. At the Advanced menu, click **Advanced Statistics** to access.

Advanced Statistics Description

Name	Description
Statistics	**Advanced Statistics**: This information pertains to how the adapter communicates with an access point. **Association**: If the adapter finds an access point to communicate with, the value is in range. Otherwise, the value is out of range. • **AP MAC Address**: The twelve-digit MAC address (`00:40:96:31:1C:05`) of the access point. • **Number of associations**: The number of times the access point has found the adapter. • **AP count**: The number of available access points within range of the WiFi adapter. • **Number of full scans**: The number of times the adapter has scanned all channels for receiving information. • **Number of partial scans**: The number of scans that have been terminated. **Roaming**: This information contains counters that are related to reasons for the adapter roaming. Roaming occurs when an adapter communicates with one access point and then communicates with another for better signal strength. • **Roaming count**: The number of times that roaming occurred. • **AP did not transmit**: The adapter did not receive radio transmission from the access point. You may need to reset the access point. • **Poor beacon quality**: The signal quality is too low to sustain communication with the access point. Either you

	have moved the adapter outside the coverage area of the access point or the access point's device address information has been changed. • **AP load balancing**: The access point ended its association with the adapter based on the access point's inability to maintain communication with all its associated adapters. Too many adapters are trying to communicate with one access point. • **AP RSSI too low**: The Receive Signal Strength Indicator (RSSI) is too low to maintain an association with the adapter. You may have moved outside the coverage area of the access point or the access point could have increased its data rate. • **Poor channel quality**: The quality of the channel is low and caused the adapter to look for another access point. • **AP dropped mobile unit**: The access point dropped a computer from the list of recognizable mobile devices. The computer must re-associate with an access point. **Miscellaneous**: Use this information to determine if an association with a different access point increases performance and helps maintain the highest possible data rate. • **Received beacons**: Number of beacons received by the adapter. • **Percent missed beacons**: Percent value for missed beacons. • **Percent transmit errors**: The percentage of data transmissions that had errors. • **Signal Strength**: Signal strength of the access point that the adapter communicates with displayed in decibels (dBm).
Transmit/Receive (Tx/Rx) Statistics	Displays percent values for non-directed and directed packets. **Total host packets**: The total number of directed and non-directed packets counts. • Transmit - (Mbps) • Receive - (Mbps) • **Non-directed packets**: The number of received packets broadcast to the wireless network. • **Directed packets**: The number of received packets sent specifically to the WiFi adapter. • **Total Bytes**: The total number of bytes for packets

	received and sent by the WiFi adapter.
Logging	Set the duration that you want to record statistical data for your WiFi adapter. **Configure logging settings**: Click **Settings** to set how frequently you want to log the statistics. You can set the number of seconds and how many hours you want the statistics to be logged. To change the storage location of the log file. 1. Click **Browse** to specify a new log file location. The current path is displayed. The default location is in the Intel PROSet/Wireless WiFi program files directory. 2. Click **Open** to close and apply the new file path. 3. Click **Close** to exit Advanced Statistics. **Start/Stop Logging**: Click this button to start and stop logging. When you click Start logging, statistical information (described above) is accumulated. When you click Stop Logging, the accumulation ends and this information is saved to a file that you can open and view. **View Log File...**: Click this button to open the Wireless folder under Program Files\Intel (this is the default location). Log files are named using the month, day, and year, plus the number of the log created on that day. For example: 03122007_001.htm. The log file provides: • Date and Time • Adapter Information • Connection Information • Transmit/Receive Statistics **NOTE**: An administrator can disable this feature.
Reset Stats	Resets the adapter statistical counters back to zero and begins making new data measurements.
Close	Closes and returns to the main window.
Help?	Provides help information for this page.

For information about importing/exporting user-created profiles, see Import or Export Profiles.

[Back to Contents](#)

Advanced Settings

Use the **Advanced Settings** to password protect a profile, select a specific access point on a network to connect to, start an application or auto import a profile. Click the **Advanced** button on the **Create WiFi Profile General Settings** to access.

Name	Description
Auto Connect	**Automatic (Default)**: Select to have the Intel(R) PROSet/ Wireless WiFi Connection Utility connect automatically to this profile when it is in range. **On Demand**: Select to prevent automatic connection of a profile when the network is in range. For example, if there is a cost for a wireless connection and you did not want to connect automatically when in range. In the WiFi Networks list and in the Profiles list, the network will be noted with this icon,  indicating On Demand connection (also called manual connection). To connect to the network: 1. Select the network from the WiFi Networks list. 2. Click **Connect**.
Auto Import	Allows a network administrator to easily move the selected profile to other computers. When the exported file is placed in the **WiFi\AutoImport** directory on another computer, the WiFi connection utility automatically imports the profile. **NOTE**: This feature is *only* available when configuring a user profile. It is *not* available when configuring Administrator Profiles.

Band Selection	Here you can select the band to use for this connection profile: • **Mixed Band (default)** : Select this to the have WiFi connection utility attempt to connect this profile to an available network with either of the two bands. • **2.4 GHz band**: Select this to have the WiFi connection utility attempt to connect this profile to an available network using only the 2.4 GHz band. • **5.2 GHz band**: Select this to have the WiFi connection utility attempt to connect this profile to an available network using only the 5.2 GHz band.
Mandatory Access Point	Forces the WiFi adapter to connect to an access point that uses a specific MAC address. Enter the MAC address of the access point (BSSID); 48-bit, 12 hexadecimal digits. For example, 00:06:25:0E:9D:84. **Clear**: Clear current address. **NOTE**: This feature is not available when ad hoc operating mode is used.
Password Protection	1. **Password protect this profile (maximum 10 characters)**: Select to enable a password for the profile. The default setting is cleared for no profile password. 2. **Password**: Enter a password. The entered password characters display as asterisks. 3. **Confirm Password**: Reenter the password. **NOTE**: Be sure to keep this password written down. If it is forgotten, it cannot be reset.
Application Auto Launch	Automatically starts a batch file, executable file, or script whenever you connect to the profile. For example, you might want a Virtual Private Network (VPN) session to start automatically whenever you connect to a wireless network. 1. Click **Enable Application Auto Launch**. 2. Enter the name of the program that you want to start or click **Browse** to locate the file on your hard disk. 3. Click **OK** to close the Advanced Settings.

Maintain Connection	The Maintain Connection option maintains the wireless connection with a user profile after log off. If the **Maintain Connection** option is selected and a Persistent profile exists, the Persistent profile will not be applied at logoff. It will be applied only if the connection with this profile is lost. **NOTE**: This option may be used with Nortel VPN client when it is configured to Logoff on Connect. **NOTE**: This feature is *only* available when configuring a user profile. It is *not* available when configuring Administrator Profiles.
User Name Format	**User Name Format**: An administrator can select the user name format for the authentication server. The choices are: • user (default) • user@domain • user@domain.com • DOMAIN\user **NOTE**: This feature is available *only* when configuring Administrator Profiles. It is not available when creating a profile from the Create WiFi Profile page.
PLC Domain Check	**Pre-logon Domain Check**: This setting is visible *only* when using the Administrator Tool, and *only* if you select to create a Pre-logon/Common profile. The choices are: • **Check for Domain Server Presence**: When using a Pre-logon Connect profile while joined to a domain, this setting will verify the domain server's presence before the user login process is finished. If the server is not found, login may be delayed for a minute or more. • **Just continue with login**: Login proceeds normally. Server presence is not checked. **NOTE**: This feature is available *only* when configuring Administrator Profiles. It is not available when creating a profile from the Create WiFi Profile page.
OK	Close and save the settings.
Cancel	Close and cancel any changes.
Help?	Help information for this page.

Back to Top

Back to Contents

Back to Contents

Profile Management

NOTE: This section describes profiles created with Intel(R) PROSet/Wireless WiFi Connection Utility. These profiles are not used by Microsoft Windows XP Wireless Zero Configuration.

What is a Profile?

A profile is a saved group of network settings. Profiles are displayed in the Profiles List. Profiles are useful when moving from one wireless network to another. Different profiles can be configured for each wireless network. Profile settings include the network name (SSID), operating mode, and security settings.

A profile is created when you connect to a wireless network.

1. Select a network from the **WiFi Networks** list.
2. Click **Connect**.
3. If the wireless network requires a WEP password or encryption key, you are prompted to enter this information prior to connection. To change the security options, click **Advanced** to open the **Create WiFi Profile Security Settings**.
4. Click **OK** to connect. A profile is created and added to the Profiles list.

The Create WiFi Profile Wizard guides you through the settings required to connect with the wireless network. At completion, the profile is saved and added to the Profiles list. Since these wireless settings are saved, the next time you are in range of this wireless network you are automatically connected.

Profile Types

There are two basic types of profiles that can be used to connect to a wireless network. The profile types are:

- **User Profiles**: These profiles are created by individual users. If there is more than one user on a computer, each user needs to create their own set of user profiles. User-created wireless profiles are not accessible by other users of a computer.
- **Administrator Profiles**: If one or more profiles need to be shared among users on a computer, the

Administrator Tool must be installed to create Administrator profiles. For more information, see [Administrator Profiles](#) .

Profiles List

The Profiles list displays a list of existing profiles. When you come in range of a wireless network, the WiFi connection utility software scans the Profiles list to see if there is a match. If a match is found, you are automatically connected to the network.



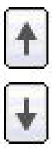
Profiles List Priority Arrows

- Use the **up-arrow** to move the position of a selected profile up in the profiles list.
- Use the **down-arrow** to move the position of a selected profile down in the profiles list.

Profile Icons

The network profile status icons indicate whether the adapter is associated with a network, the type of operating mode being used, and whether security encryption is enabled. These icons display next to the profile name in the Profiles list.

Name	Description

Profile Name	The Profile Name is your name for this network. It can be anything that helps you identify this network. For example, My Home Network, Coffee Shop on A Street.
Network Name	Name of the wireless network (SSID) or computer.
Connection Icons: The network profile status icons indicate the different connection states of the adapter with a wireless network, the type of operating mode being used, and whether network security is being used.	
	**Blue circle**: The WiFi adapter is associated with an access point or computer (Device to Device [ad hoc] mode). If a profile has 802.1X security enabled, this indicates that the WiFi adapter is associated and authenticated.
	Indicates Network (infrastructure) mode.
	Indicates Device to Device (ad hoc) mode.
	Indicates an Administrator profile.
	The wireless network uses Security encryption.
	Indicates that this network is on the Exclude list, e.g. is set for manual rather than automatic connection. When on the Exclude list, to connect the user must connect manually.
Arrows 	Use the arrows to position profiles in a preferred order for auto-connection. • **Up-arrow**: Move the position of a selected profile up in the Profiles list. • **Down-arrow**: Move the position of a selected profile down in the Profiles list.
Connect	Connect the selected profile for the wireless network.
Add	Opens the **Create WiFi Profile General Settings**, which are used to create a new profile. See Create a New Profile for more information.
Remove	Removes a selected profile from the Profiles list. See Remove a Profile for more information.
Properties	Used to edit the contents of an existing profile. You can also double-click a profile in the Profiles list to edit the profile. See Edit an Existing Profile for more information.
	**Export/Import**: Imports and exports user-based profiles to and from the Profiles list. Wireless profiles can be automatically imported into the Profiles list. See Export or Import Profiles for more information.
Close	Closes the profile management window.
Help?	Provides help information for this page.

Connect to a Profile

When you are in range of a wireless network that has a matching profile you are automatically connected to that network. If a network with a lower priority profile is also in range you can force the connection to that lower profile. This is achieved the from the WiFi connection utility or from the Taskbar icon.

Manually connect to a profile from the Intel PROSet/Wireless WiFi software:

1. Double-click the **Taskbar** icon to open the Intel PROSet/Wireless WiFi main window.
2. Click **Profiles** to open the Profiles list.
3. Select the profile from the Profiles list.
4. Click **Connect**. Remember that the connection is only made if the wireless network is in range.

Manually connect to a profile from the **Taskbar**:

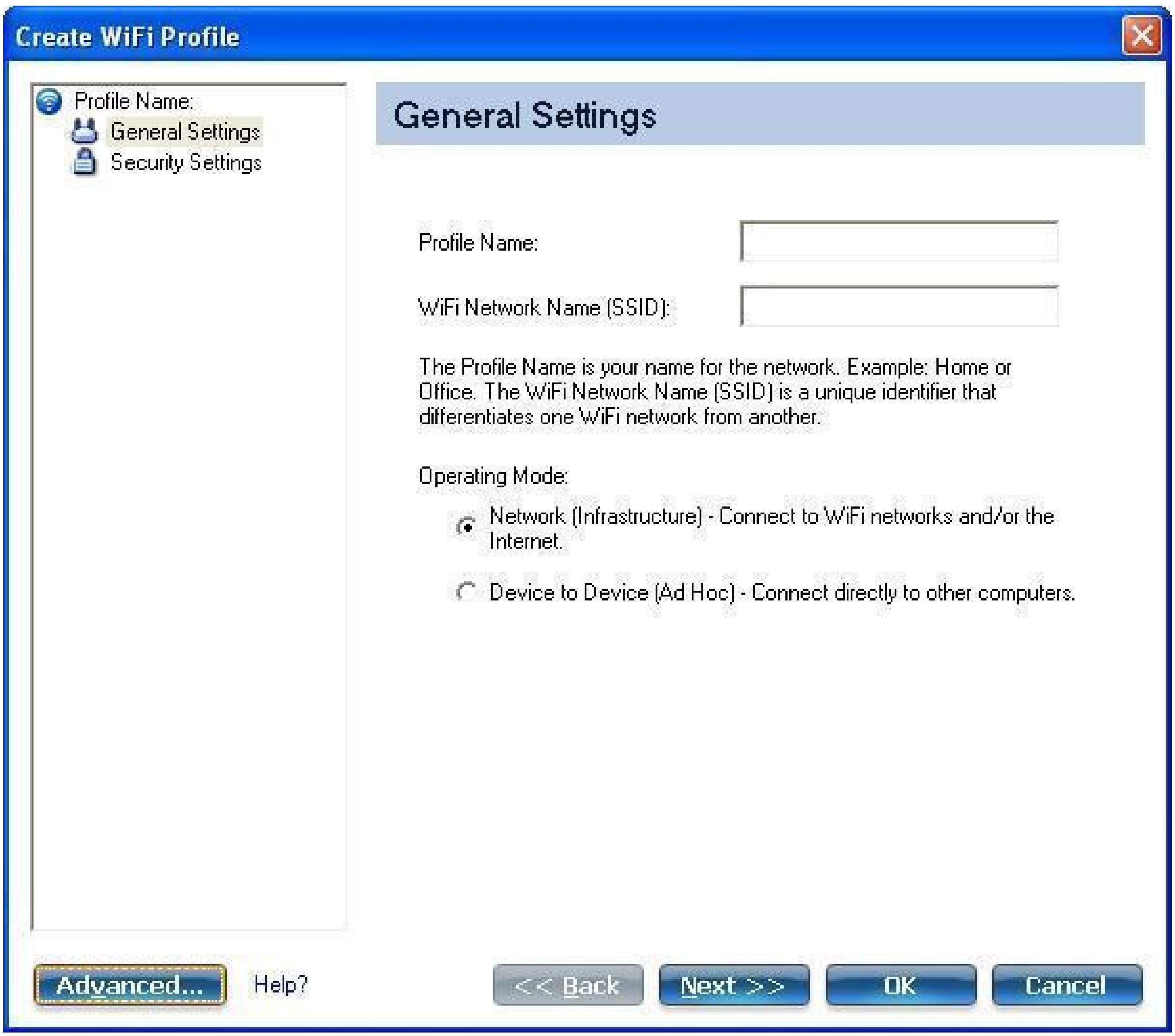
1. Right-click the Intel PROSet/Wireless WiFi Taskbar icon.
2. Click **Connect to Profile**.
3. Select a profile.
4. Click to start the connection.

Create a New Profile

Select a network from the **Wireless Networks** list. Click **Connect**. The **Create WiFi Profile** manager guides you through the necessary steps to create a profile and connect to the network. During this process, the **Create WiFi Profile Security Settings** attempts to detect the appropriate security settings for you.

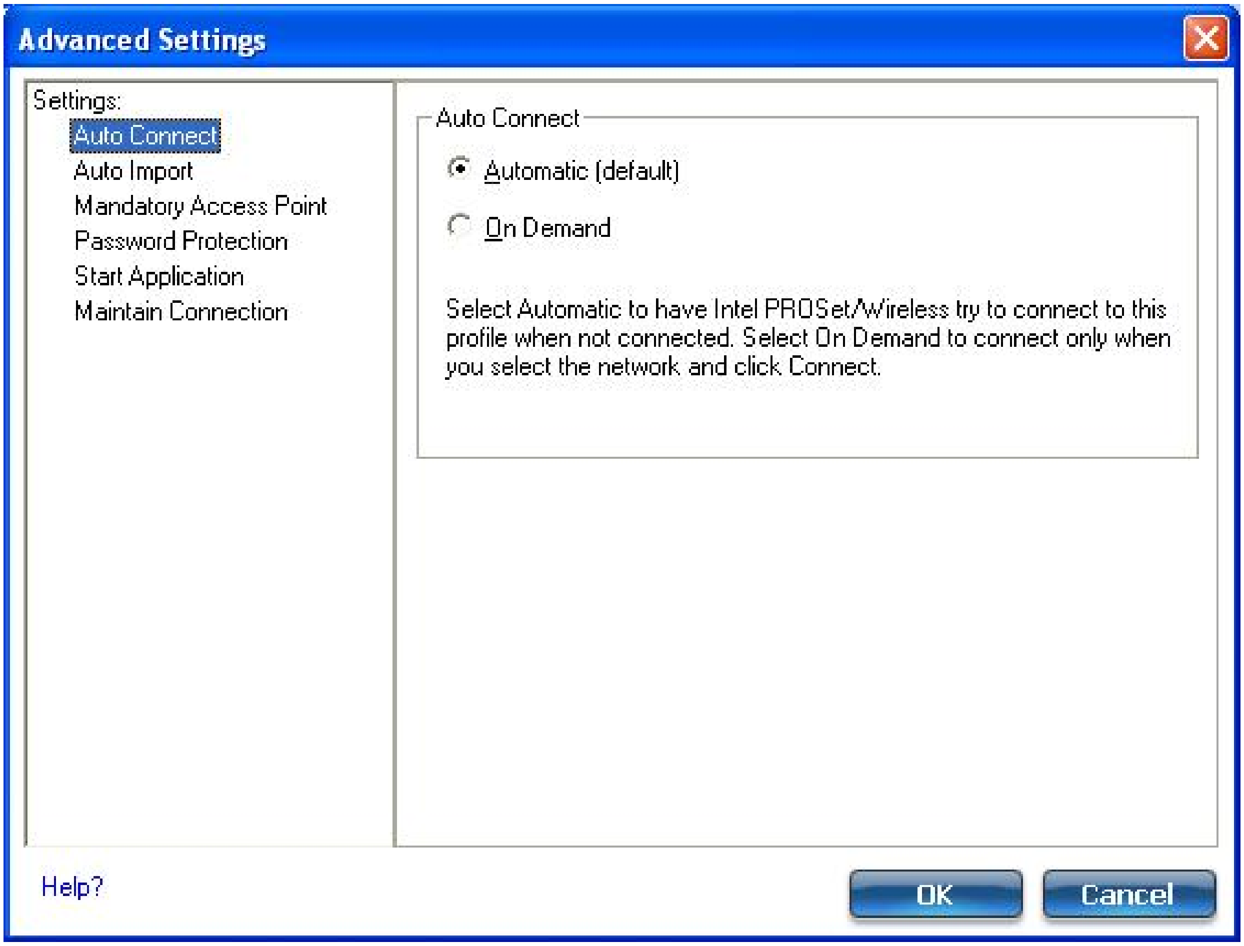
To create a new profile and connect to a wireless network:

1. From the Intel PROSet/Wireless WiFimain window, click **Profiles**.
2. On the Profiles page, click **Add** to open the **Create WiFi Profile General Settings**. (See General Settings for more information.)



3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the network name of the WiFi network

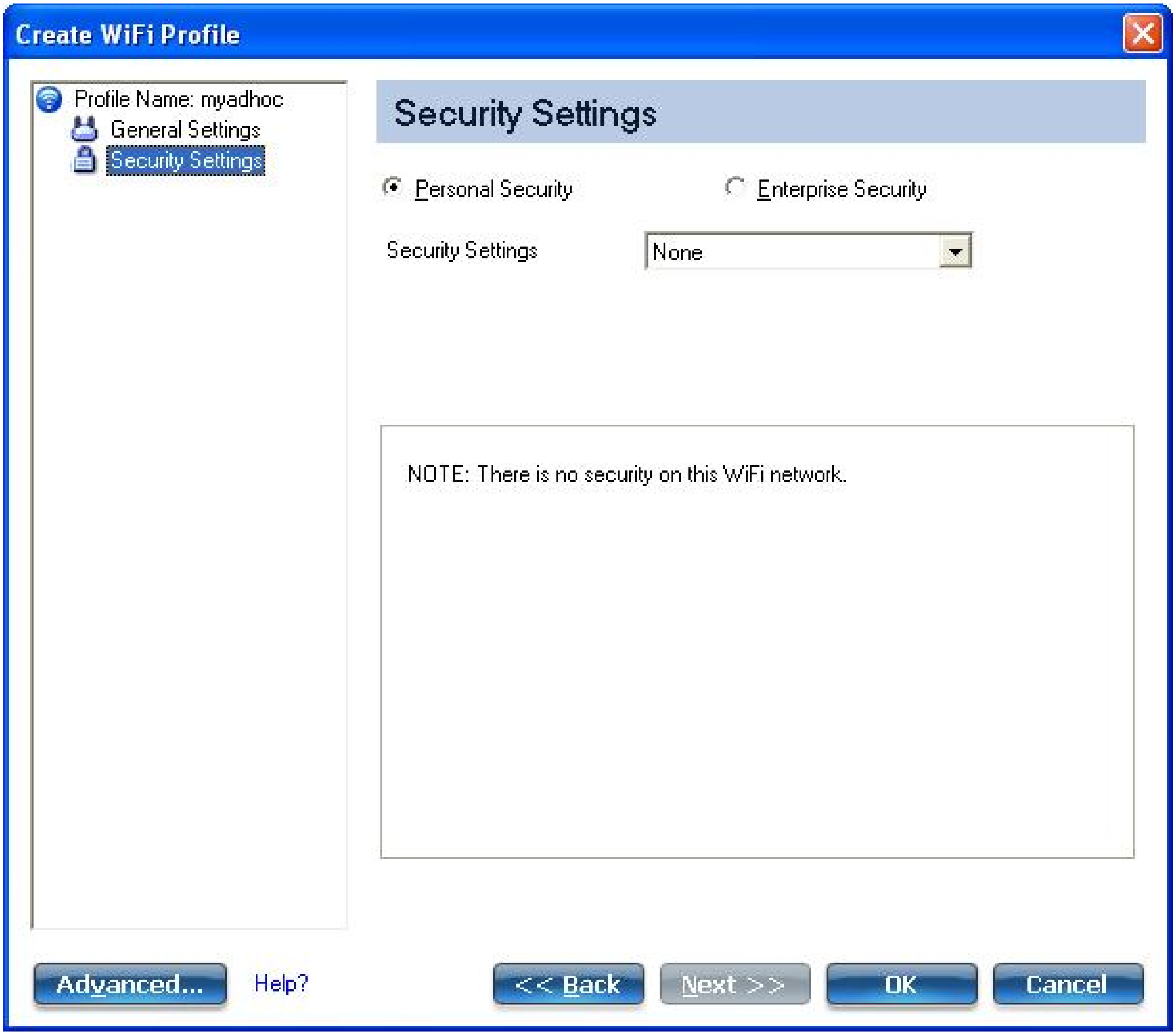
5. Select the Operating Mode: **Network (Infrastructure)** or **Device to Device (ad hoc)**.
6. Click Advanced for the following options:
   - Auto Connect: Select to automatically or manually connect to a profile.
   - Auto Import: Network administrator can export a profile on another computer.
   - Mandatory Access Point: Select to associate the WiFi adapter with a specific access point.
   - Password Protection: Select to password protect a profile.
   - Application Auto Launch: Specify a program to be started when a wireless connection is made.
   - Maintain Connection: Select to remain connected to a user profile after log off.



7. From the General Settings, click **Next** to open the Security Settings.



8. Select either Personal or Enterprise Security to select the **Network Authentication** and **Data Encryption** options. Enter the encryption key settings and configure the 802.1X settings as required.



9. Click **OK** when you have completed the profile settings. To change or verify the profile settings, click **Back**.
10. If you are not currently connected to a network, Intel PROSet/Wireless WiFi detects that a new profile has been added and automatically attempts to connect to this new profile.
11. If you want to manually connect to this profile, click **Connect**. The connection icon displays the current connection status. The network name, transmit and receive speeds, and signal quality are also displayed.

Edit an Existing Profile

To edit an existing profile:

1. Click **Profiles** on the Intel PROSet/Wireless WiFi main window.
2. Select the profile to edit from the Profiles List.
3. Click **Properties** to open the **WiFi Profile Properties General Settings**.
4. Click **Next** and **Back** to navigate through the WiFi Profile Properties' General and Security Settings:
   - **General Settings**: See General Settings for more information.
   - **Security Settings**: See Security Settings for more information.
5. Click **OK** to save the current settings and exit. Click **Cancel** to exit without saving changes.

Remove a Profile

To remove a profile:

1. Click **Profiles** on the Intel PROSet/Wireless WiFi main window.
2. Select the profile from the list.
3. Click **Remove**. You are notified that **Selected profiles will be permanently removed. Do you want to continue?**
4. Click **Yes**. The profile is removed from the Profiles list.

If you are still connected to the network:

1. Click **Profiles** on the Intel PROSet/Wireless WiFi main window.
2. Select the profile from the list.
3. Click **Remove**. You are notified that **Selected profiles will be permanently removed. Do you want to continue?**
4. Click **Yes**. You are notified that **<profile name> is active and will be permanently removed. Do you want to continue?**
5. Click **Yes**. The profile is removed from the Profiles list.

NOTE: If the profile is protected by a password, you cannot remove or edit the profile settings without entering the password. If the administrator or you do not know the password, there is no process available to reset the password.

Set a Profile Password

To password protect an existing profile:

1. Click **Profiles** on the Intel PROSet/Wireless WiFimain window.
2. Select the profile from the list.
3. Click **Properties** to open the WiFi Profile Properties' General Settings.
4. Click **Advanced** to open the Advanced Settings.
5. Click **Password Protection** to open the Password Protection settings.
6. Click **Password protect this profile (maximum 10 characters)**
7. **Password**: Enter the password.
8. **Confirm Password**: Reenter the password.
9. Click **OK** to save the setting and return to the General Settings page.
10. Click **OK** to return to the Intel PROSet/Wireless WiFi main window.

Import or Export Profiles

This feature lets you import and export user-based profiles to and from the Profiles list. Wireless profiles can be automatically imported into the Profiles list.

An administrator can set profiles to be imported automatically into the Profiles list. Intel PROSet/Wireless WiFi monitors the import folder on your hard disk for new profile files. Only profiles that have been enabled through **Enable Auto-Import** in the Advanced Settings are automatically imported. If a profile of the same name already exists in the Profiles list, you are notified to either reject the imported profile or accept it. If accepted, the existing profile is replaced. All imported user-based profiles are placed at the bottom of the Profiles List.

NOTE: To export Administrator profiles, see Administrator Packages.



Import Profiles into the Profiles List

To import profiles manually:

1. Click **Import** on the Profiles page.
2. Select the profile files to import.
3. Click **Import**.
4. You are notified that the profile has been successfully imported.

Export Profiles from the Profiles List

1. Select individual or multiple profiles from the list.
2. Select **Export** to export one or more profiles from the Profiles list.
3. Select the destination folder. Click **Browse** to search your hard disk for the destination directory. The C:\ drive is the default directory.
4. Click **OK** to export the selected profile. You are notified: **Successfully exported selected profiles to the destination folder: C:**.

To select multiple profiles:

1. Use your mouse to highlight a profile.
2. Press **Ctrl**.
3. Click each profile that you want selected. Follow the instructions from Step 2 above to export multiple profiles.

Password Protected Profiles

Import and export password-protected user-based profiles automatically to remote systems. If a profile is password protected, the assigned password must be entered before it can be edited. See Set a Profile Password for more information.

Back to Top

Back to Contents

Back to Contents

Profile Wizard General Settings

The **General Settings** page is the first page in the Create WiFi Profile Wizard. From this page you can specify the profile name, the WiFi Network Name (SSID), and choose the operating mode.

See Profile Management for a description of when the Create WiFi Profile General Settings is launched.

While you configure a profile, you can use the left pane to navigate to the General and Security Settings pages. The **Back** and **Next** buttons located at the bottom of the Profile Wizard can also be used for the same functions.

General Settings Page Description

Name	Description
Profile Name	Name of the wireless network profile. When you configure a wireless network that was selected from the WiFi Networks list, the profile name is the same as the WiFi Network Name SSID). This name can be changed to be more descriptive or customized for your personal use. Examples: My Office Network, Bob's Home Network, ABC Company Network
WiFi Network Name (SSID)	Name of the wireless network access point used by the WiFi adapter for connection. The network name must match exactly the name of the wireless access point. It is case sensitive. When you configure a wireless network that was selected from the WiFi Networks list, the network name is taken from the wireless network list. You cannot and should not change it. **<SSID not broadcast>**: If an access point does not broadcast its network name (SSID) or the WiFi adapter receives a hidden network name from a stealth access

	point, it is displayed in the WiFi Networks list. To associate with an <SSID not broadcast> network entry, a new profile must be created before connection. Provide the actual SSID for the access point. After connection, the <SSID not broadcast> is still displayed in the WiFi Networks list. The associated SSID profile is viewed in the Profiles list.
Operating Mode	**Network (Infrastructure)**: Connect to an access point. An Infrastructure network consists of one or more access points and one or more computers with WiFi adapters. This connection is the type used in home networks, corporate networks, hotels, and other areas that provide access to the network and/or the internet. **NOTE**: Only **Network (Infrastructure)** is available for administrator profiles (Pre-logon/Common and Persistent profiles). See the Administrator Tool for more information. **Device to Device (ad hoc)**: Connect directly to other computers in an ad hoc wireless network. This type of connection is useful for connections between two or more computers only. It does not provide access to network resources or the internet.
Administrator Profile Type (Visible only in Administrator Tool)	**Persistent**: Persistent profiles are applied at boot time or whenever no one is logged on the computer. After a user logs off, a Persistent profile maintains a wireless connection either until the computer is turned off, or a different user logs on. **Pre-logon/Common**: These profiles are only available using the Administrator Tool. Pre-logon/Common profiles are applied once a user logs on. The connection is made as part of the Windows log-on sequence (Pre-logon/Common). This profile is shared by all users.
Advanced	Click **Advanced** to access the Advanced Settings. Use the Advanced Settings to set Maintain Connection, User Name Format, Auto Connect or Auto Import options, launch an application (Application Auto Launch), set a profile password (Password Protection), specify a certain access point address for adapter connection (Mandatory Access Point), and set Pre-logon Connect options.

Next	Proceeds to the Security Settings page.
OK	Finishes creation of the new profile with the current settings.
Cancel	Closes the Create WiFi Profile Wizard and cancel any changes.
Help?	Provides help information for this page.

Back to Top

Back to Contents

[Back to Contents](#)

Exclude List Management

The Exclude list is a list of networks that you will not automatically be connected to. This feature lets you restrict automatic access to a listed network or access point, even if you have created a profile for that network. Use **Exclude List Management** to exclude entire WiFi networks (SSID).

There are two ways to access the Exclude List Management screen:

- Click **Manage Exclusions** at the Profiles menu, or
- At the main window, select a network and click the Properties button. Then click **Manage Exclusions**.

NOTE: If an administrator has designated a network for exclusion, only an administrator using the Administrator Tool may remove the network from the Exclude List. Administrators can exclude profiles from the Administrator Tool. See Administrator Tool.

This icon on the WiFi Networks list indicates that a network has been excluded. 

Name	Description
Network Name	Name (SSID) of the wireless network.
Radio	Displays the band if there is a DHCP error.
MAC Address	The MAC address of the access point, or all access points or stations in the network.
Reason	The source of the exclusion, the User.

<table>
<tr><td>Details</td><td>Click Details to learn specific information on how the access point was excluded and how to remove it from exclusion. Following is an example:

This network has been excluded from automatic connection for the following reasons.
User has excluded this network manually.
To make this network (or access points) eligible for automatic connection again, select it and click the Remove button.

NOTES:
The Reset list button removes all entries except rogue and administrator excluded access points from the list.
Rogue access points are removed from the list when a connection is made to this access point using valid credentials.
All excluded access points in a network (other than rogue and administrator excluded) are removed from the list when a profile for that network is applied manually.
Entries that are dimmed are excluded rogue or administrator excluded access points. Rogue or administrator excluded access points cannot be removed from the list manually.</td></tr>
<tr><td>Add</td><td>Click the Add button to enter the network name (SSID) that you want to add to the Exclude List.
Network Name: Enter the network name.
Click OK.</td></tr>
<tr><td>Remove</td><td>Remove an entry from the list.
Select the entry from the list.
Click Remove.
You are asked: Do you want to remove the selected item from the Exclude List?
Click Yes to remove the profile from the list.</td></tr>
<tr><td>Reset list</td><td>Removes all of the networks and access points from the Exclude List.</td></tr>
<tr><td>Close</td><td>Closes and saves settings.</td></tr>
<tr><td>Help?</td><td>Provides help information for this page.</td></tr>
</table>

Back to Top

Back to Contents

Trademarks and Disclaimers

Back to Content

Set Up Profile Security

Network Authentication

802.1X Authentication Types

Use the Intel(R) PROSet/Wireless WiFi Connection Utility

The following sections describe how to use the WiFi connection utility to set up the required security settings for your WiFi adapter. See Personal Security.

It also provides information about how to configure advanced security settings for your WiFi adapter. This requires information from a systems administrator (corporate environment) or advanced security settings on your access point (for home users). See Enterprise Security.

For general information about security settings, See Security Overview.

Set up Data Encryption and Authentication

In a home wireless network you can use a variety of simple security procedures to protect your wireless connection. These include:

- Enable Wi-Fi Protected Access* (WPA).
- Change your password.
- Change the network name (SSID).

Wi-Fi Protected Access (WPA) encryption provides protection for your data on the network. WPA uses an encryption key called a pre-shared key (PSK) to encrypt data before transmission. Enter the same password in all of the computers and access point in your home or small business network. Only devices that use the same encryption key can access the network or decrypt the encrypted data transmitted by other computers. The password automatically initiates the Temporal Key Integrity Protocol (TKIP) or AES-CCMP protocol for the data encryption process.

Network Keys

WEP encryption provides two levels of security:

- 64-bit key (sometimes referred to as 40-bit)
- 128-bit key (also known as 104-bit)

For improved security, use a 128-bit key. If you use encryption, all wireless devices on your wireless network must use the same encryption keys.

You can create the key yourself and specify the key length (64-bit or 128-bit) and key index (the location that a specific key is stored). The greater the key length, the more secure the key.

Key Length: 64-bit

Pass phrase (64-bit): Enter five (5) alphanumeric characters, 0-9, a-z or A-Z.
Hex key (64-bit): Enter 10 hexadecimal characters, 0-9, A-F.

Key Length: 128-bit

Pass phrase (128-bit): Enter 13 alphanumeric characters, 0-9, a-z or A-Z.
Hex key (128-bit): Enter 26 hexadecimal characters, 0-9, A-F.

With WEP data encryption, wireless station can be configured with up to four keys (the key index values are 1, 2, 3, and 4). When an access point or a wireless station transmits an encrypted message that uses a key stored in a specific key index, the transmitted message indicates the key index that was used to encrypt the message body. The receiving access point or wireless station can then retrieve the key that is stored at the key index and use it to decode the encrypted message body.

Set up a Client with No Authentication and No Data Encryption

CAUTION: Networks using no authentication or encryption are highly vulnerable to access by unauthorized users.

On the WiFi connection utility main page, select one of the following methods to connect to an infrastructure network:

- Double-click an infrastructure network in the WiFi Networks list.
- Select an infrastructure network in the WiFi Networks list. Click **Connect**. The WiFi connection utility automatically detects the security settings for the WiFi adapter.

If there is no authentication required, the network connects without a prompt to enter any log-on credentials. Any wireless device with the correct network name (SSID) is able to associate with other devices in the network.

To create a profile for a WiFi network connection with no encryption:

1. Click **Profiles** on the WiFi connection utility main window.
2. On the Profiles list, click **Add** to open the wireless profile **General Settings**.
3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the name of your wireless network.
5. **Operating Mode**: Click **Device to Device (ad hoc)**.
6. Click **Next** to open the **Security Settings**.
7. **Personal Security** is selected by default.
8. **Security Settings**: The default setting is **None**, which indicates that there is no security on this wireless network.
9. Click **OK.** The profile is added to the Profiles list and connects to the wireless network.

Set up a Client with WEP 64-bit or WEP 128-bit Data Encryption

When WEP data encryption is enabled, a network key or password is used for encryption.

A network key is provided for you automatically (for example, it might be provided by your wireless network adapter manufacturer), or you can enter it yourself and specify the key length (64-bit or 128-bit), key format (ASCII characters or hexadecimal digits), and key index (the location where a specific key is stored). The greater the key length, the more secure the key.

To add a network key for a Device to Device (ad hoc) network connection:

1. On the WiFi connection utility main window, double-click a Device to Device (ad hoc) network in the WiFi Networks list or select the network and click **Connect**.
2. Click **Profiles** to access the Profiles list.
3. Click **Properties** to open the wireless profile **General Settings**. The Profile name and WiFi Network Name (SSID) display. **Device to Device (ad hoc)** should be selected as the Operating Mode.
4. Click **Next** to open the **Security Settings**.
5. **Personal Security** is selected by default.
6. **Security Settings**: The default setting is **None**, which indicates that there is no security on this wireless network.

To add a password or network key:

1. **Security Settings**: Select either **WEP 64-bit** or **WEP 128-bit** to configure WEP data encryption with a 64-bit or 128-bit key.

   When WEP encryption is enabled on an access point, the WEP key is used to verify access to the network. If the wireless device does not have the correct WEP key, even though authentication is successful, the device is unable to transmit data through the access point or decrypt data received from the access point.

Name	Description
Password	Enter the Wireless Security Password (Pass phrase) or Encryption Key (WEP key).
Pass phrase (64-bit)	Enter five (5) alphanumeric characters, 0-9, a-z or A-Z.

WEP key (64-bit)	Enter 10 hexadecimal characters, 0-9, A-F.
Pass phrase (128-bit)	Enter 13 alphanumeric characters, 0-9, a-z or A-Z.
WEP key (128-bit)	Enter 26 hexadecimal characters, 0-9, A-F.

2. **Key Index**: Change the Key Index to set up to four passwords.
3. Click **OK** to return to the Profiles list.

To add more than one password:

1. Select the Key Index number: **1, 2, 3,** or **4**.
2. Enter the Wireless Security Password.
3. Select another Key Index number.
4. Enter another Wireless Security Password.

Set up a Client with WPA*-Personal (TKIP) or WPA2*-Personal (TKIP) Security Settings

WPA* Personal Mode requires manual configuration of a pre-shared key (PSK) on the access point and clients. This PSK authenticates a user's password or identifying code, on both the client station and the access point. An authentication server is not needed. WPA Personal Mode is targeted to home and small business environments.

WPA2* is the second generation of WPA security that provides enterprise and consumer wireless users with a high level of assurance that only authorized users can access their wireless networks. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government users.

NOTE: To achieve transfer rates greater than 54 Mbps on 802.11n connections, WPA2-AES security must be selected. No security (**None**) can be selected to enable network setup and troubleshooting.

To configure a profile with WPA-Personal network authentication and TKIP data encryption:

1. On the WiFi connection utility main window, double-click an infrastructure network in the WiFi Networks list or select the network and click **Connect**.
2. Click **Profiles** to access the Profiles list.
3. Click **Properties** to open the wireless profile **General Settings**. The Profile name and

WiFi Network Name (SSID) display. **Network (Infrastructure)** should be selected as the Operating Mode.

4. Click **Next** to open the **Security Settings**.
5. Select **Personal Security**.
6. **Security Settings**: Select **WPA-Personal (TKIP)** to provide security to a small business network or home environment. A password, called a pre-shared key (PSK), is used. The longer the password, the stronger the security of the wireless network.

   If your wireless access point or router supports WPA2-Personal, then you should enable it on the access point and provide a long, strong password. The longer the password, the stronger the security of the wireless network. The same password entered in the access point needs to be used on this computer and all other wireless devices that access the wireless network.

   NOTE: WPA-Personal and WPA2-Personal are interoperable.

7. **Wireless Security Password (Encryption Key)**: Enter a text phrase with eight to 63 characters. Verify that the network key matches the password in the wireless access point.
8. Click **OK** to return to the Profiles list.

Set up a Client with WPA*-Personal (AES-CCMP) or WPA2*-Personal (AES-CCMP) Security Settings

Wi-Fi Protected Access (WPA*) is a security enhancement that strongly increases the level of data protection and access control to a wireless network. WPA enforces 802.1X authentication and key-exchange and only works with dynamic encryption keys. For a home user or small business, WPA-Personal uses either Advanced Encryption Standard - Counter CBC-MAC Protocol (AES-CCMP) or Temporal Key Integrity Protocol (TKIP).

NOTE: For the Intel(R) Wireless WiFi Link 4965AGN adapter, to achieve transfer rates greater than 54 Mbps on 802.11n connections, WPA2-AES security must be selected. No security (**None**) can be selected to enable network setup and troubleshooting.

To create a profile with WPA2*-Personal network authentication and AES-CCMP data encryption:

1. On the WiFi connection utility main window, double-click an infrastructure network from the WiFi Networks list or select the network and click **Connect**.
2. If these are being transmitted, the Profile name and WiFi Network Name (SSID) should display on the **General Settings** screen. **Network (Infrastructure)** should be selected as the Operating Mode. Click **Next** to open the **Security Settings**.
3. Select **Personal Security**.

4. **Security Settings**: Select **WPA2-Personal (AES-CCMP)** to provide this level of security in the small network or home environment. It uses a password, also called a pre-shared key (PSK). The longer the password, the stronger the security of the wireless network.

   AES-CCMP (Advanced Encryption Standard - Counter CBC-MAC Protocol) is a newer method for privacy protection of wireless transmissions specified in the IEEE 802.11i standard. AES-CCMP provides a stronger encryption method than TKIP. Choose AES-CCMP as the data encryption method whenever strong data protection is important.

   If your Wireless access point or router supports WPA2-Personal, then you should enable it on the access point and provide a long, strong password. The same password entered into the access point needs to be used on this computer and all other wireless devices that access the wireless network.

   NOTE: WPA-Personal and WPA2-Personal are interoperable.

   Some security solutions may not be supported by your computer's operating system. You may require additional software or hardware as well as wireless LAN infrastructure support. Contact your computer manufacturer for details.

5. **Password: Wireless Security Password (Encryption Key)**: Enter a text phrase (length is between eight and 63 characters). Verify that the network key used matches the wireless access point key.
6. Click **OK** to return to the Profiles list.

Back to Top

Back to Contents

Back to Contents

Configure Profiles for Network (Infrastructure) Operating Mode

---

A Network (Infrastructure) network consists of one or more access points and one or more computers with WiFi adapters installed. Each access point must have a wired connection to a wireless network. This section describes how to create various profiles.

Create a Windows XP* Profile with No Authentication or Data Encryption (None)

CAUTION: Networks using no authentication or encryption are highly vulnerable to access by unauthorized users.

To create a profile for a WiFi network connection with no encryption:

1. Click **Profiles** on the Intel(R) PROSet/Wireless WiFi Connection Utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list/tab, click **Add** to open the **Create WiFi Profile General Settings**.
3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the network identifier.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security** to open the **Security Settings**.
9. **Network Authentication: Open** (Selected).

   Open authentication allows a wireless device access to the network without 802.11 authentication. If no encryption is enabled on the network, any wireless device with the

correct network name (SSID) can associate with an access point and gain access to the network.

10. **Data Encryption**: **None** is the default.
11. Click **OK**. The profile is added to the Profiles list and connects to the wireless network.

Create a Windows XP* Profile with Shared Network Authentication

When *shared key* authentication is used, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel. Shared key authentication requires that the client configure a static WEP or CKIP key. The client access is granted only if it passes a challenge-based authentication. CKIP provides stronger data encryption than WEP, but not all operating systems and access points support it.

NOTE: While shared key would appear to be the better option for a higher level of security, a known weakness is created by the clear text transmission of the challenge string to the client. Once an invader sniffs for the challenge string, the shared authentication key can be easily reverse engineered. Therefore, open authentication (with data encryption) is actually, and counter intuitively, more secure.

To create a profile with shared authentication:

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the [Administrator Tool].
2. On the Profiles list/tab, click **Add** to open the **Create WiFi Profile General Settings**.
3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the network identifier.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select [Persistent] or [Pre-logon/Common]. (This step applies only if you are using the Administrator Tool.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **Shared**. Shared authentication is accomplished with a pre-configured WEP key.
10. **Data Encryption**: Select None, WEP (64-bit or 128-bit), or CKIP (64-bit or 128-bit).
11. **Enable 802.1X**: Disabled.
12. **Encryption Level**: **64-bit or 128-bit**: When switching between 64-bit and 128-bit encryption, the previous settings are erased and a new key must be entered.
13. **Key Index**: Select **1**, **2**, **3**, or **4**. Change the Key Index to specify up to four passwords.
14. **Wireless Security Password (Encryption Key)**: Enter the wireless network password (Encryption Key). This password is the same value used by the wireless access point or router. Contact your administrator for this password.
    - **Pass phrase (64-bit)**: Enter five (5) alphanumeric characters, 0-9, a-z or A-Z.
    - **Hex key (64-bit)**: Enter 10 hexadecimal characters, 0-9, A-F.
    - **Pass phrase (128-bit)**: Enter 13 alphanumeric characters, 0-9, a-z or A-Z.
    - **Hex key (128-bit)**: Enter 26 hexadecimal characters, 0-9, A-F.

Create a Windows XP* Profile with WPA-Personal or WPA2-Personal

Network Authentication

Wi-Fi Protected Access (WPA) is a security enhancement that strongly increases the level of data protection and access control to a wireless network. WPA-Personal enforces key-exchange and only works with dynamic encryption keys. If your wireless access point or router supports WPA-Personal or WPA2-Personal, then you should enable it on the access point and provide a long, strong password. For personal or home networks without a RADIUS or AAA server, use Wi-Fi Protected Access Personal.

- **WPA-Personal**: A wireless security method that provides strong data protection and prevents unauthorized network access for small networks. It uses Temporal Key Integrity Protocol (TKIP) or AES-CCMP encryption and protects against unauthorized network access through the use of a pre-shared key (PSK).
- **WPA2-Personal**: A follow-on wireless security method to WPA that provides stronger data protection and prevents unauthorized network access for small networks.

NOTE: WPA-Personal and WPA2-Personal are interoperable.

Some security solutions may not be supported by your computer's operating system and may require additional software or certain hardware as well as wireless LAN infrastructure support. Check with your computer manufacturer for details.

To add a profile with WPA-Personal or WPA2-Personal network authentication:

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list/tab, click **Add** to open the **Create WiFi Profile General Settings**.
3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the network identifier.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **WPA-Personal or WPA2-Personal**. See Security Overview.
10. **Data Encryption**: Select either TKIP or AES-CCMP.
11. **Password**: Enter a text phrase from 8 to 63 characters. The longer the password, the stronger the security of the wireless network. The same password entered into an access points needs to be used on this computer and all other wireless devices that access the wireless network.

Create a Windows XP* Profile with WPA-Enterprise or WPA2-Enterprise Network Authentication

WPA2-Enterprise requires an authentication server.

- **WPA-Enterprise**: A wireless security method that provides strong data protection for multiple users and large managed networks. It uses the 802.1X authentication framework with TKIP or AES-CCMP encryption and prevents unauthorized network access by verifying network users through an authentication server.
- **WPA2-Enterprise**: The follow-on wireless security method to WPA that provides stronger data

protection for multiple users and large managed networks. It prevents unauthorized network access by verifying network users through an authentication server.

NOTE: WPA-Enterprise and WPA2-Enterprise are interoperable.

To add a profile that uses WPA-Enterprise or WPA2-Enterprise authentication:

1. Obtain a user name and password on the RADIUS server from your administrator.
2. Certain Authentication Types require that you obtain and install a client certificate. See Create a Profile with TLS authentication or consult your administrator.
3. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
4. On the Profiles list, click **Add** to open the **Create WiFi Profile General Settings**.
5. **Profile Name**: Enter a descriptive profile name.
6. **WiFi Network Name (SSID)**: Enter the network identifier.
7. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
8. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)
9. Click **Next** to open the **Security Settings**.
10. Click **Enterprise Security**.
11. **Network Authentication**: Select **WPA-Enterprise** or **WPA2-Enterprise**.
12. **Data Encryption**: Select either TKIP or AES-CCMP.
13. **Enable 802.1X**: Selected by default.
14. **Authentication Type**: Select one of the following: EAP-SIM, LEAP, TLS, TTLS, PEAP, or EAP-FAST.

Configure a Network Profile with 802.1X Authentication Types

Create a Windows XP* Profile with WEP Data Encryption and EAP-SIM Network Authentication

EAP-SIM uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. EAP-SIM requires you to enter a user verification code, or PIN, for communication with the Subscriber Identity Module (SIM) card. A SIM card is a special smart card that is used by Global System for Mobile Communications (GSM) based digital cellular networks.

To add a profile with EAP-SIM authentication:

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list, click **Add** to open the **Create WiFi Profile General Settings**.
3. **Profile Name**: Enter a profile name.
4. **WiFi Network Name (SSID)**: Enter the network identifier.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Pre-logon/Common. (This step applies only if you are using the Administrator Tool. EAP-SIM cannot be used for Persistent profiles.)

7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **Open** (Recommended).
10. **Data Encryption**: Select **WEP**.
11. Click **Enable 802.1X**.
12. **Authentication Type**: Select EAP-SIM.

EAP-SIM authentication can be used with:

- **Network Authentication types**: Open, Shared, WPA-Enterprise and WPA2-Enterprise
- **Data Encryption types**: None, WEP, TKIP, AES-CCMP and CKIP

EAP-SIM User (optional)

1. Click **Specify user name (identity)**:
2. At **User Name**: Enter the user name assigned to the SIM card.
3. Click **OK**.

Create a Windows XP* Profile with EAP-AKA Network Authentication

EAP-AKA (Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement) is an EAP mechanism for authentication and session key distribution, using the Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (USIM). The USIM card is a special smart card used with cellular networks to validate a given user with the network.

EAP-AKA authentication can be used with:

- **Network Authentication types**: Open, WPA-Enterprise and WPA2-Enterprise
- **Data Encryption types**: WEP or CKIP for Open authentication, TKIP or AES-CCMP for Enterprise authentication.

EAP-AKA uses Enterprise Security and for network authentication, can use Open, WPA Enterprise, or WPA2 Enterprise.

To add a profile with EAP-AKA authentication:

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list, click **Add** to open the **Create WiFi Profile General Settings**.
3. **Profile Name**: Enter a profile name.
4. **WiFi Network Name (SSID)**: Enter the network identifier.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Pre-logon/Common. (This step applies only if you are using the Administrator Tool. EAP-SIM cannot be used for Persistent profiles.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **Open**, **WPA-Enterprise**, or **WPA2-Enterprise**.
10. **Data Encryption**: Select **WEP** or **CKIP** for **Open** authentication, **TKIP** or **AES-CCMP** for **Enterprise** authentication.

11. Click **Enable 802.1X** if it is not already selected.
12. **Authentication Type**: Select **EAP-AKA**.

EAP-AKA User (optional)

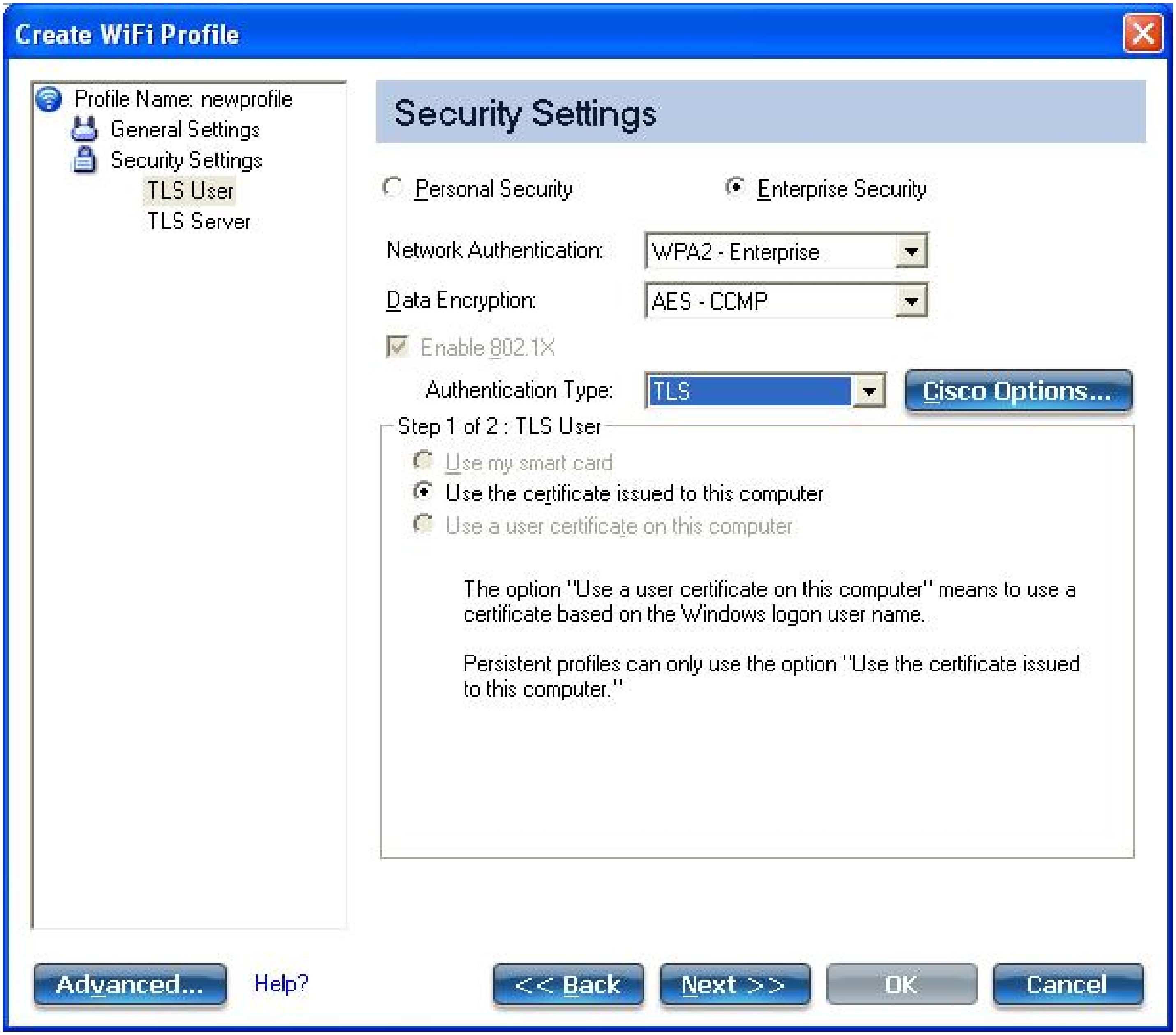
1. Click **Specify user name (identity)**:
2. At **User Name**: Enter the user name assigned to the USIM card.
3. Click **OK**.

Create a Windows XP* Profile with TLS Network Authentication

These settings define the protocol and the credentials used to authenticate a user. Transport Layer Security (TLS) authentication is a two-way authentication method that exclusively uses digital certificates to verify the identity of a client and a server.

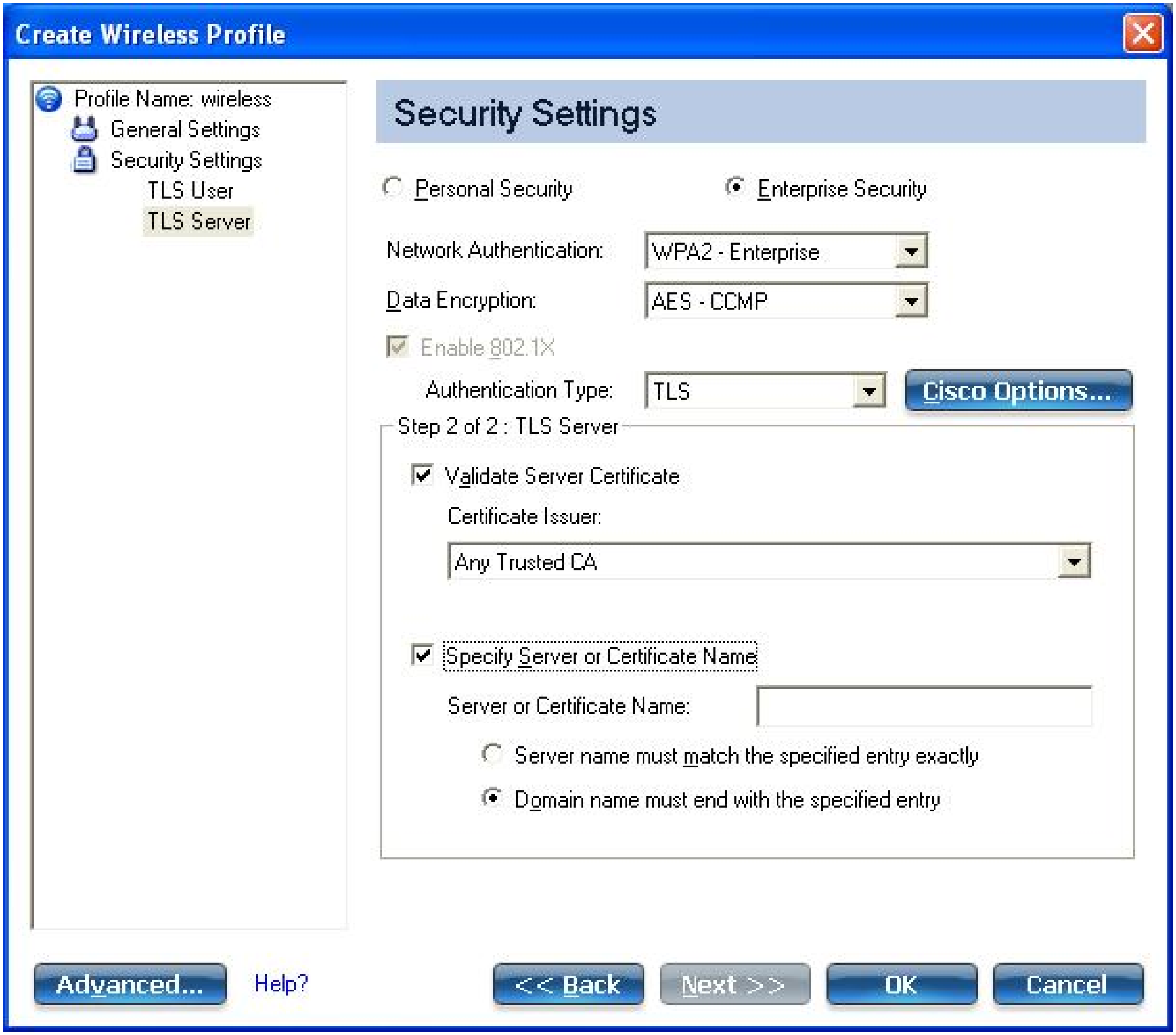
To add a profile with TLS authentication:

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list, click **Add** to open the **Create WiFi Profile General Settings**.
3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the network identifier.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **WPA-Enterprise** or **WPA2-Enterprise** (Recommended).
10. **Data Encryption**: Select **AES-CCMP** (Recommended).
11. **Enable 802.1X**: Selected by default.
12. **Authentication Type**: Select **TLS** to be used with this connection.



Step 1 of 2: TLS User

1. Obtain and install a client certificate. See Create a Profile with TLS authentication or consult your system administrator.
2. Select one of the following to obtain a certificate: Use my smart card, Use the certificate issued to this computer, or Use a user certificate on this computer.
3. Click **Next** to open the **TLS Server** settings.



Step 2 of 2: TLS Server

1. Select one of the following credential retrieval methods: Validate Server Certificate or Specify Server or Certificate Name.
2. Click **OK**. The profile is added to the Profiles list.
3. Click the new profile at the end of the Profiles list. Use the up and down arrows to change the priority of the new profile.
4. Click **Connect** to connect to the selected wireless network.
5. Click **OK** to close Intel PROSet/Wireless WiFi.

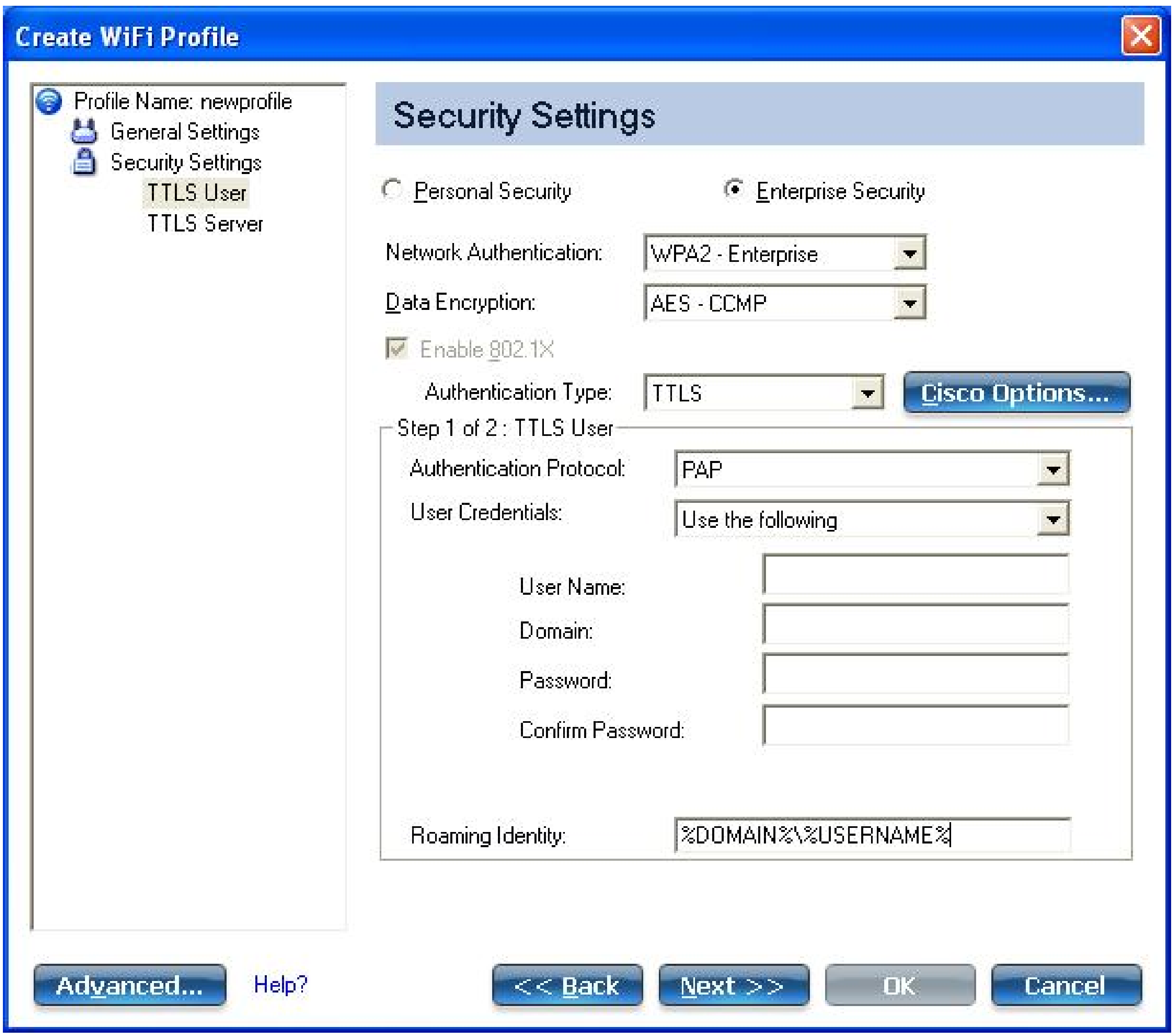
Create a Windows XP* Profile with TTLS Network Authentication

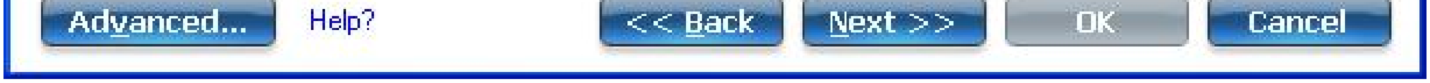
TTLS authentication: These settings define the protocol and credentials used to authenticate a user. The client uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client can use another authentication protocol. Typically password-based protocols challenge

over a non-exposed TLS encrypted channel.

To set up a client with TTLS Authentication:

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list, click **Add** to open the **Create WiFi Profile General Settings**.
3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the network identifier.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **WPA-Enterprise** or **WPA2-Enterprise** (Recommended)
10. **Data Encryption**: Select **TKIP** or **AES-CCMP** (Recommended).
11. **Enable 802.1X**: Selected by default.
12. **Authentication Type**: Select **TTLS** to be used with this connection.



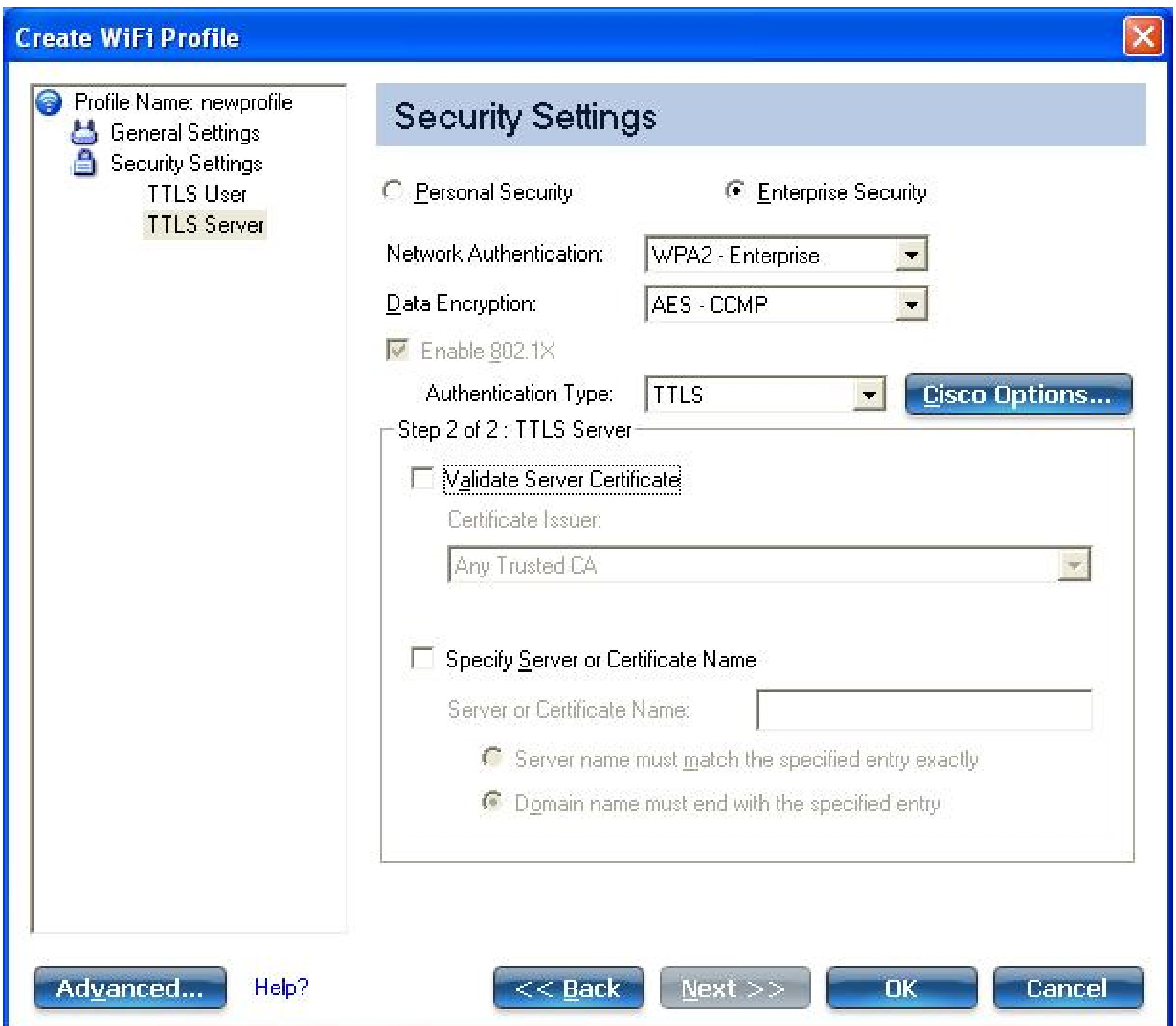


Step 1 of 2: TTLS User

1. **Authentication Protocol**: This parameter specifies the authentication protocol operating over the TTLS tunnel. The protocols are: PAP (Default), CHAP, MS-CHAP and MS-CHAP-V2. See Security Overview for more information.
2. **User Credentials**: For PAP, CHAP, MS-CHAP, and MS-CHAP-V2 protocols, select one of these authentication methods: Use Windows logon, Prompt each time I connect, or Use the following.
3. **Roaming Identity**: A Roaming Identity may be populated in this field or you can use %domain%\%username% as the default format for entering a roaming identity.

   When 802.1X Microsoft IAS RADIUS is used as an authentication server, the server authenticates the device using the **Roaming Identity** from Intel PROSet/Wireless WiFi software, and ignores the **Authentication Protocol MS-CHAP-V2** user name. Microsoft IAS RADIUS accepts only a valid user name (dotNet user) for the Roaming Identity. For all other authentication servers, the Roaming Identity is optional. Therefore, it is recommended to use the desired realm (for example, anonymous@myrealm) for the Roaming Identity rather than a true identity.

4. Click **Next** to access the TTLS Server settings.





Step 2 of 2: TTLS Server

1. Select one of the following credential retrieval methods: Validate Server Certificate or Specify Server or Certificate Name.
2. Click **OK** to save the setting and close the page.

Create a Windows XP* Profile with PEAP Network Authentication

PEAP authentication: PEAP settings are required for the authentication of the client to the authentication server. The client uses EAP-TLS to validate the server and create a TLS-encrypted channel between client and server. The client can use another EAP mechanism, such as Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2, over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel. The following example describes how to use WPA with AES-CCMP or TKIP encryption with PEAP authentication.

To set up a client with PEAP Authentication: Obtain and install a client certificate. See Create a Windows XP* Profile for TLS authentication or consult your administrator.

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list, click **Add** to open the **Create WiFi Profile General Settings**.
3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the network identifier.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **WPA-Enterprise** or **WPA2-Enterprise** (Recommended).
10. **Data Encryption**: Select one of the following: AES-CCMP is recommended.
11. **Enable 802.1X**: Selected by default.
12. **Authentication Type**: Select **PEAP** to be used with this connection.

Step 1 of 2: PEAP User

PEAP relies on Transport Layer Security (TLS) to allow unencrypted authentication types such as EAP-Generic Token Card (GTC) and One-Time Password (OTP) support.

1. **Authentication Protocol**: Select either GTC, MS-CHAP-V2 (Default), or TLS. See Authentication Protocols.
2. **User Credentials**: Select one of the following: Use Windows logon, Prompt each time I connect, or Use the following.
3. **Roaming Identity**: A Roaming Identity may be populated in this field or you can use %domain%\%username% as the default format for entering a roaming identity.

When 802.1X Microsoft IAS RADIUS is used as an authentication server, the server authenticates the device using the **Roaming Identity** from Intel PROSet/Wireless WiFi software, and ignores the **Authentication Protocol MS-CHAP-V2** user name. Microsoft IAS RADIUS accepts only a valid user name (dotNet user) for the Roaming Identity. For all other authentication servers, the Roaming Identity is optional. Therefore, it is recommended to use the desired realm (for example, anonymous@myrealm) for the Roaming Identity rather than a true identity.

Configure Roaming Identity to Support Multiple Users:

If you use a Pre-logon/Common profile that requires the roaming identity to be based on the Windows logon credentials, the creator of the profile can add a roaming identity that uses %username% and %domain%. The roaming identity is parsed and the appropriate log on information is substituted for the keywords. This allows maximum flexibility in configuring the roaming identity while allowing multiple users to share the profile.

Please see your authentication server user guide for directions about how to format a suitable roaming identity. Possible formats are:

%domain%\%user_name%
%user_name%@%domain%
%user_name%@%domain%.com
%user_name%@mynetwork.com

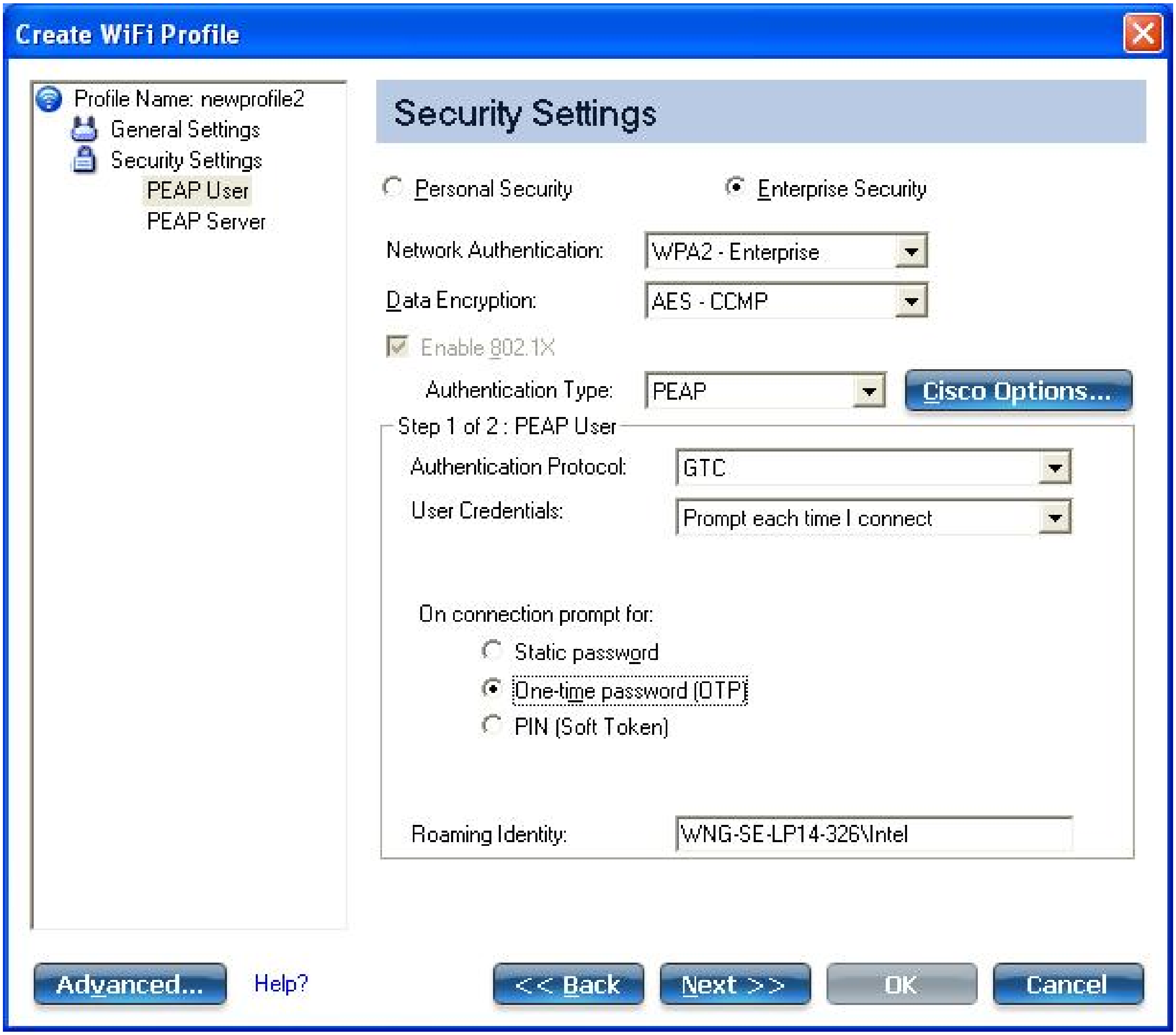
If Roaming Identity is blank, %domain%\%username% is the default.

Notes about the credentials: This user name and domain must match the user name that is set in the authentication server by the administrator prior to client authentication. The user name is case-sensitive. This name specifies the identity supplied to the authenticator by the authentication protocol operating over the TLS tunnel. This user identity is securely transmitted to the server only after an encrypted channel has been verified and established.

Authentication Protocols

This parameter specifies the authentication protocols that can operate over the TTLS tunnel. Next are instructions on how to configure a profile that uses PEAP authentication with GTC, MS-CHAP-V2 (Default), or TLS authentication protocols.

Generic Token Card (GTC)



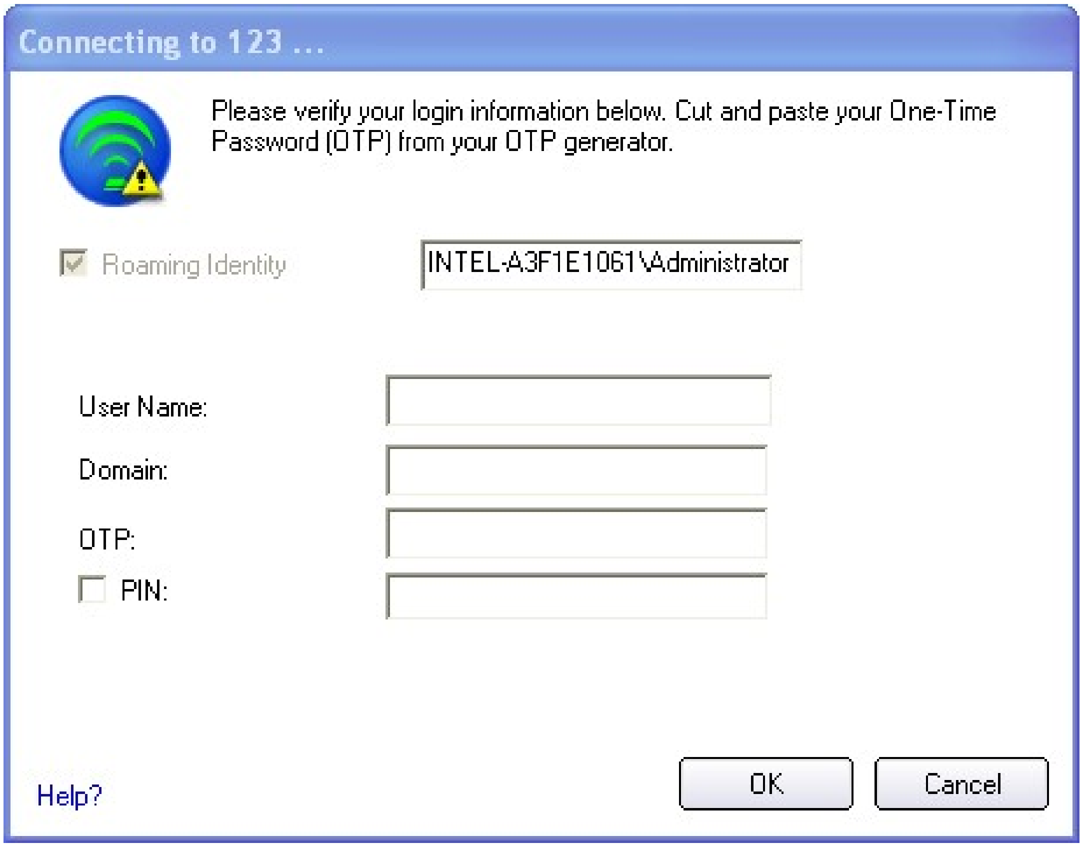
To configure a one-time password:

1. **Authentication Protocol**: Select **GTC** (Generic Token Card).
2. **User Credentials**: Select **Prompt each time I connect**. (This is only available if you are creating a personal profile. Not available for IT profiles.)
3. **On connection prompt for**: Select one of the following:

Name	**Description**
Static Password	On connection, enter the user credentials.
One-time password (OTP)	Obtain the password from a hardware token device.
PIN (Soft Token)	Obtain the password from a soft token program.

NOTE: The **Prompt each time I connect** option is unavailable if an Administrator has cleared the **Cache Credentials** setting in the Administrator Tool. See Administrator Application Settings for more information.

4. Click **OK**.
5. If you are acting as the user, perform the following three steps.
6. Select the profile on the WiFi Networks list.
7. Click **Connect**. When prompted, enter the user name, domain and OTP.
8. Click **OK**. You are asked to verify your log in information.



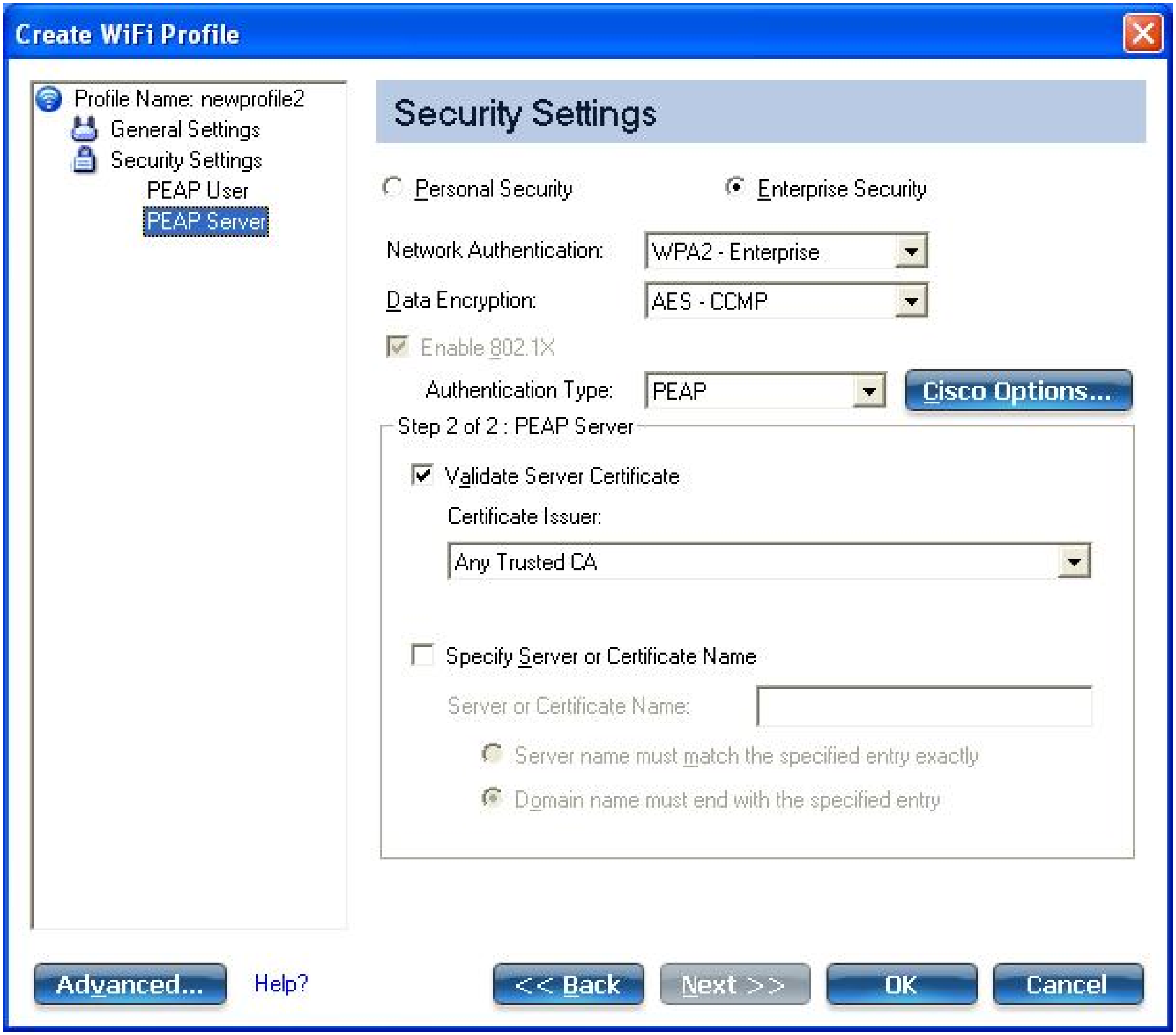
MS-CHAP-V2: This parameter specifies the authentication protocol operating over the PEAP tunnel.

1. **User Credentials**: Select one of the following options: Use Windows logon, Prompt each time I connect, or Use the following.
2. Click **Next** to open the PEAP Server settings.

TLS: Transport Layer Security authentication is a two-way authentication method that exclusively uses digital certificates to verify the identity of a client and a server.

1. Obtain and install a client certificate. See Create a Windows XP* Profile for TLS authentication or consult your system administrator.
2. Select one of the following to obtain a certificate: Use my smart card, Use the certificate issued to this computer, or Use a user certificate on this computer.
3. Click **Next** to open the PEAP Server settings.

Step 2 of 2: PEAP Server



1. Select one of the following credential retrieval methods: Validate Server Certificate or Specify Server or Certificate Name.
2. Click **OK**. The profile is added to the Profiles list.
3. Click the new profile at the end of the Profiles list. Use the up and down arrows to change the priority of the new profile.
4. Click **Connect** to connect to the selected wireless network.

   If you did not select **Use Windows logon** on the Security Settings page and also did not configure user credentials, no credentials are saved for this profile. Please enter your credentials to authenticate to the network.

5. Click **OK** to close Intel PROSet/Wireless WiFi.

PEAP-TLS Certificate Auto Enrollment

In the Application Settings, select **Enable TLS rejected certificates notification** if you want a warning issued when a PEAP-TLS certificate is rejected. When a certificate has an invalid field expiration date, you

are notified that you must take one of the following actions:

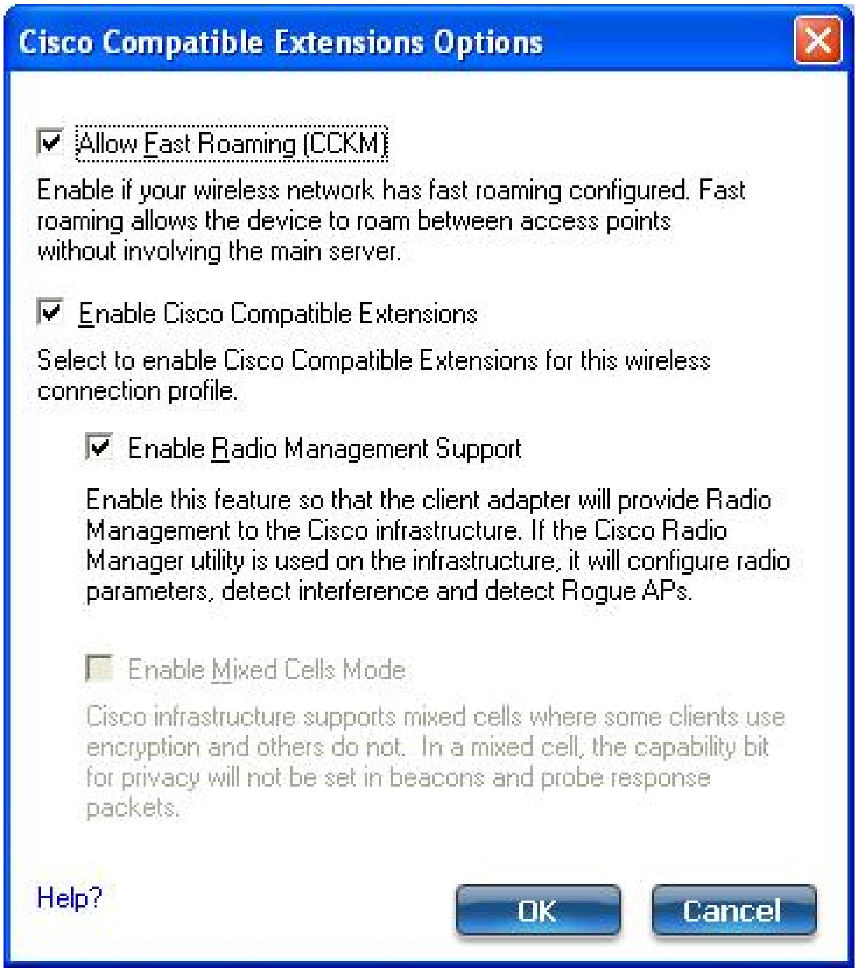
> **A potential authentication problem for profile has been detected. The expiration date in the associated certificate may be invalid. Choose one of the following options**:

Control	**Description**
Continue with current parameters.	Continue with the current certificate.
Update certificate manually.	The Select Certificate page opens for you to choose another certificate.
Update certificate automatically based on the certificates in the local store.	This option is enabled only when the local store holds one or more certificates for which the "issued to" and "issued by" fields match the current certificate and for which the "expiration date" has not expired. If you choose this option, the application selects the first valid certificate.
Log off to obtain certificate during logon process (this does not update the profile and only applies to certificates configured for auto enrollment).	Logs off the user, who must obtain a proper certificate during the next logon process. The profile must be updated to select the new certificate.
Auto enrollment	You are notified to: **Please wait while the system is trying to obtain the certificate automatically**. Click **Cancel** to end the certificate retrieval.
Do not show this message again.	A user is able to avoid this step in subsequent sessions. The choice selected is remembered for future sessions.

Create a Windows XP* Profile with LEAP Network Authentication

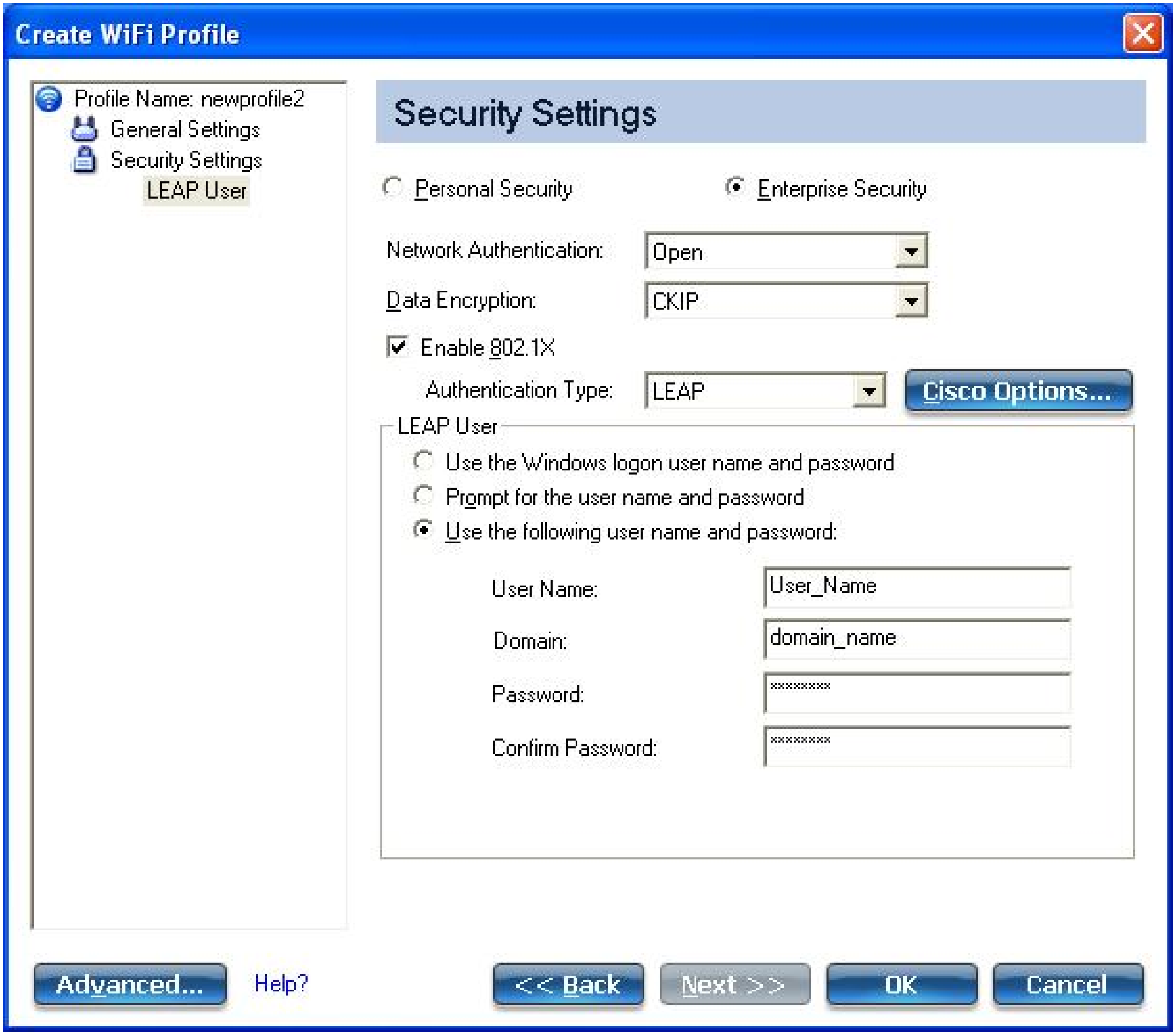
Cisco LEAP (Light Extensible Authentication Protocol) is an 802.1X authentication type that supports strong mutual authentication between the client and a RADIUS server. The LEAP profiles settings include LEAP, CKIP with Rogue access point detection integration. To set up a client with LEAP authentication:

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list, click **Add**. The **Create WiFi Profile General Settings** opens.
3. **Profile Name**: Enter a descriptive profile name.
4. **WiFi Network Name (SSID)**: Enter the network identifier.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **WPA-Enterprise** or **WPA2-Enterprise** (Recommended).
10. **Data Encryption**: AES-CCMP is recommended.
11. **Enable 802.1X**: Selected by default.
12. **Authentication Type**: Select **LEAP** to be used with this connection.
13. Click **Cisco Options**.
14. Click Enable Cisco Compatible Extensions to enable Cisco Compatible Extensions (CCX) security (Allow Fast Roaming (CCKM), Enable Radio Management Support, and Enable Mixed Cells Mode).



15. Click **Enable Radio Management Support** to detect rogue access points.
16. Click **OK** to return to the Security Settings.

LEAP User:



1. Select one of the following authentication methods listed next. If under **Administrator Profile Type** you selected **Persistent** (with or without selecting Pre-logon/Common), then only Use the following user name and password is available. If you *only* selected **Pre-logon/Common**, then the following three authentication methods are available.
   - Use the Windows logon user name and password
   - Prompt for the user name and password
   - Use the following user name and password
2. Click **OK** to save the setting and close the page.

Create a Windows XP* Profile with EAP-FAST Network Authentication

In Cisco Compatible Extensions, Version 3 (CCXv3), Cisco added support for EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling), which uses protected access

credentials (PACs) to establish an authenticated tunnel between a client and a server.

Cisco Compatible Extensions, Version 4 (CCXv4) improves the provisioning methods for enhanced security and provides innovations for enhanced security, mobility, quality of service, and network management.

Cisco Compatible Extensions, Version 3 (CCXv3)

To set up a client with EAP-FAST authentication with Cisco Compatible Extensions, version 3 (CCXv3):

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list, click **Add** to open the **Create WiFi Profile General Settings**.
3. **WiFi Network Name (SSID)**: Enter the network identifier.
4. **Profile Name**: Enter a descriptive profile name.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **WPA-Enterprise** or **WPA2-Enterprise** (Recommended).
10. **Data Encryption**: AES-CCMP is recommended.
11. **Enable 802.1X**: Selected by default.
12. **Authentication Type**: Select **EAP-FAST** to be used with this connection.

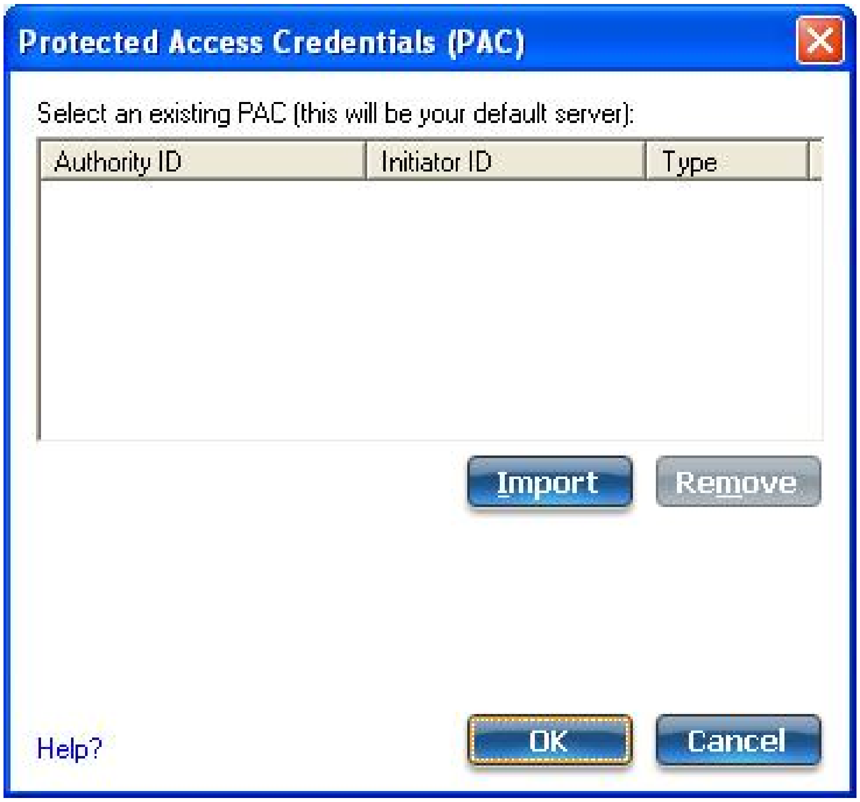
    NOTE: If CCXv4 Application Setting was not installed through an Administrator Package, only EAP-FAST User Settings are available for configuration. See EAP-FAST User Settings.

Step 1 of 2: EAP-FAST Provisioning

1. Click **Disable EAP-FAST Enhancements (CCXv4)** to allow provisioning inside a server-unauthenticated TLS tunnel (Unauthenticated-TLS-Server Provisioning Mode).
2. Click **Select server** to view any unauthenticated PACs that have already been provisioned and reside on this computer.

    NOTE: If the provisioned PAC is valid, the WiFi connection utility does not prompt the user for acceptance of the PAC. If the PAC is invalid, WiFi connection utility fails the provisioning automatically. A status message is displayed in the Wireless Event Viewer that an administrator can review on the user's computer.

3. To import a PAC:



a. Click **Select server** to open the Protected Access Credentials (PAC) list.
b. Click **Import** to import a PAC that resides on this computer or a server.
c. Select the PAC and click **Open**.
d. Enter the PAC password (optional).
e. Click **OK** to close this page. The selected PAC is added to PAC list.

4. Click **Next** to select the credential retrieval method or click **OK** to save the EAP-FAST settings and return to the Profiles list. The PAC is used for this wireless profile.

Step 2 of 2: EAP-FAST Additional Information

To perform client authentication in the established tunnel, a client sends a user name and password to authenticate and establish client authorization policy.

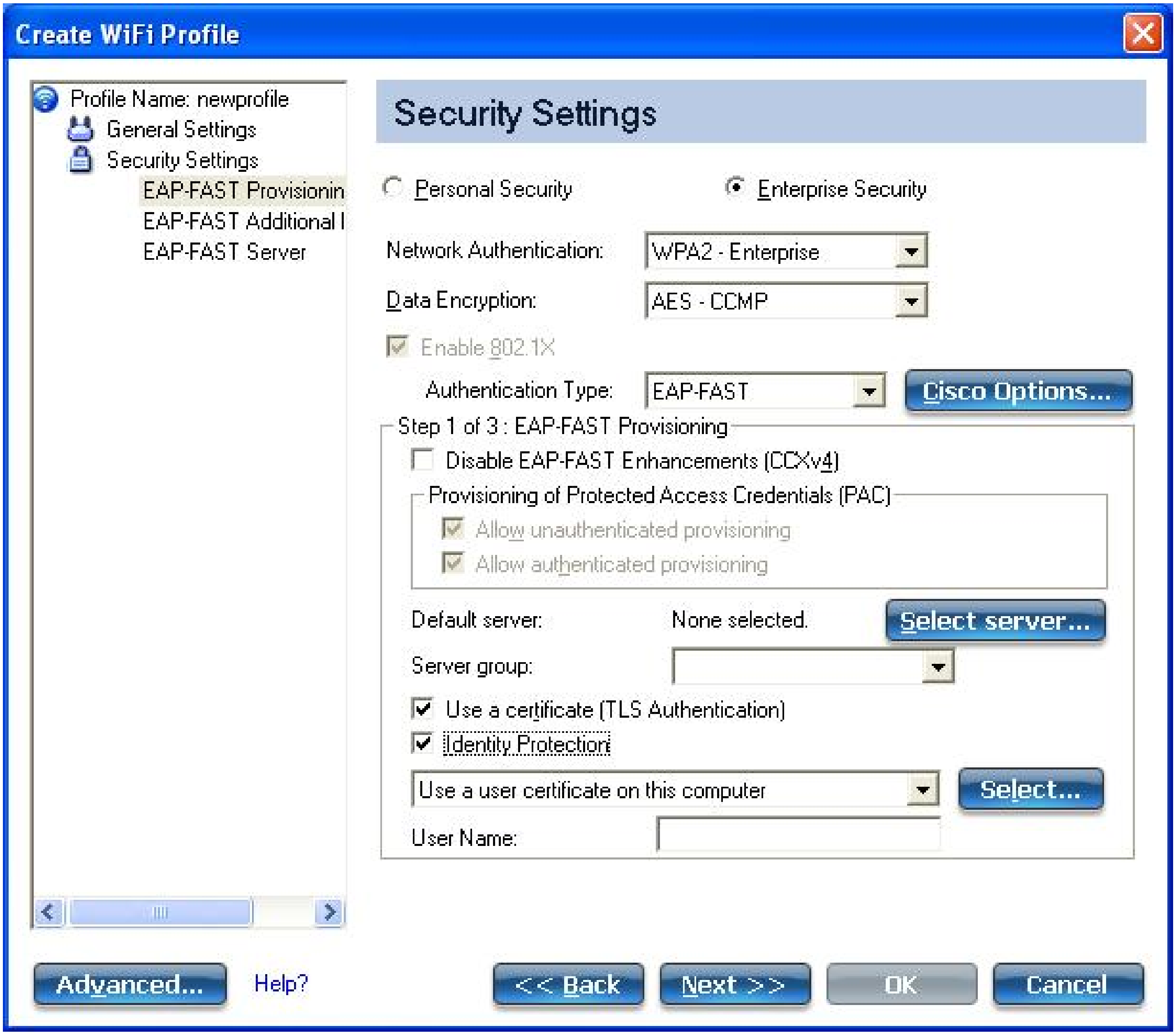
1. Click **User Credentials** to select one of the following credentials retrieval method: Use Windows logon, Prompt each time I connect, or Use the following.
2. Click **OK** to save the settings and close the page. Server verification is not required.

Cisco Compatible Extensions, Version 4 (CCXv4)

To set up a client with EAP-FAST authentication with Cisco Compatible Extensions, version 4 (CCXv4):

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profiles list, click **Add** to open the **Create WiFi Profile General Settings**.
3. **WiFi Network Name (SSID)**: Enter the network identifier.
4. **Profile Name**: Enter a descriptive profile name.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)

7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **WPA-Enterprise** or **WPA2-Enterprise** (Recommended).
10. **Data Encryption**: AES-CCMP is recommended.
11. **Enable 802.1X**: Selected.
12. **Authentication Type**: Select **EAP-FAST** to be used with this connection.



Step 1 of 3: EAP-FAST Provisioning

With CCXv4, EAP-FAST supports two modes for provisioning:

- Server-Authenticated Mode: Provisioning inside a server authenticated TLS tunnel.
- Server-Unauthenticated Mode: Provisioning inside an unauthenticated TLS tunnel.

NOTE: Server-Authenticated Mode provides significant security advantages over Server-Unauthenticated Mode even when EAP-MS-CHAP-V2 is being used as an inner method. This mode protects the EAP-MS-CHAP-V2 exchanges from potential Man-in-the-Middle attacks by verifying the server's authenticity before exchanging MS-CHAP-V2. Therefore, Server-Authenticated Mode is preferred whenever it is possible. EAP-

FAST peer must use Server-Authenticated Mode whenever a certificate or public key is available to authenticate the server and ensure the best security practices.

Provisioning of Protected Access Credentials (PAC):

EAP-FAST uses a PAC key to protect the user credentials that are exchanged. All EAP-FAST authenticators are identified by an authority identity (A-ID). The local authenticator sends its A-ID to an authenticating client, and the client checks its database for a matching A-ID. If the client does not recognize the A-ID, it requests a new PAC.

NOTE: If the provisioned Protected Access Credential (PAC) is valid, the WiFi connection utility does not prompt the user for acceptance of the PAC. If the PAC is invalid, the WiFi connection utility fails the provisioning automatically. A status message is displayed in the Wireless Event Viewer that an administrator can review on the user's computer.

1. Verify that **Disable EAP-FAST Enhancements (CCXv4)** is not selected. **Allow unauthenticated provisioning** and **Allow authenticated provisioning** are selected by default. Once a PAC is selected from the Default Server, you can deselect any of these provisioning methods.
2. **Default Server**: **None** is selected as the default. Click **Select Server** to select a PAC from the default PAC authority server or select a server from the **Server group** list. The EAP-FAST Default Server (PAC Authority) selection page opens.

   NOTE: Server groups are only listed if you have installed an Administrator Package that contains EAP-FAST Authority ID (A-ID) Group settings.

   PAC distribution can also be completed manually (out-of-band). Manual provisioning enables you to create a PAC for a user on an ACS server and then import it into a user's computer. A PAC file can be protected with a password, which the user needs to enter during a PAC import.

3. To import a PAC:
   a. Click **Import** to import a PAC from the PAC server.
   b. Click **Open**.
   c. Enter the PAC password (optional).
   d. Click **OK** closes this page. The selected PAC is used for this wireless profile.

EAP-FAST CCXv4 enables support for the provisioning of other credentials beyond the PAC currently provisioned for tunnel establishment. The credential types supported include trusted CA certificate, machine credentials for machine authentication, and temporary user credentials used to bypass user authentication.

Use a certificate (TLS Authentication)

1. Click **Use a certificate (TLS Authentication)**
2. Click **Identity Protection** when the tunnel is protected.
3. Select one of the following to obtain a certificate: Use my smart card, Use the certificate issued to this computer, or Use a user certificate on this computer.
4. **User Name**: Enter the user name assigned to the user certificate.
5. Click **Next**.

Step 2 of 3: EAP-FAST Additional Information

If you selected **Use a certificate (TLS Authentication)** and **Use a user certificate on this computer**,

click **Next** (no roaming identity is required) and proceed to Step 3 to configure EAP-FAST Server certificate settings. If you do not need to configure EAP-FAST server settings, click **OK** to save your settings and return to the Profiles page.

If you selected to **Use my smart card**, add the roaming identity, if required. Click **OK** to save your settings and return to the Profiles page.

If you did not select **Use a certificate (TLS Authentication)**, click **Next** to select an Authentication Protocol. CCXv4 permits additional credentials or TLS cipher suites to establish the tunnel.

Authentication Protocol: Select either GTC, or MS-CHAP-V2 (Default).

Generic Token Card (GTC)

GTC may be used with Server-Authenticated Mode. This enable peers using other user databases as Lightweight Directory Access Protocol (LDAP) and one-time password (OTP) technology to be provisioned in-band. However, the replacement may only be achieved when used with the TLS cipher suites that ensure server authentication.

To configure a one-time password:

1. **Authentication Protocol**: Select **GTC** (Generic Token Card).
2. **User Credentials**: Select **Prompt each time I connect**.
3. **On connection prompt for**: Select one of the following:

Name	Description
Static Password	On connection, enter the user credentials.
One-time password (OTP)	Obtain the password from a hardware token device.
PIN (Soft Token)	Obtain the password from a soft token program.

4. Click **OK**.
5. Select the profile on the WiFi Networks list.
6. Click **Connect**. When prompted, enter the user name, domain and one-time password (OTP).
7. Click **OK**.

MS-CHAP-V2. This parameter specifies the authentication protocol operating over the PEAP tunnel.

1. **Authentication Protocol**: Select **MS-CHAP-V2**.
2. Select the user credentials: Use Windows logon, Prompt each time I connect, or Use the following.
3. **Roaming Identity**: A Roaming Identity may be populated in this field or you can use %domain%\%username% as the default format for entering a roaming identity.

   When 802.1X Microsoft IAS RADIUS is used as an authentication server, the server authenticates the device using the **Roaming Identity** from Intel PROSet/Wireless WiFi software, and ignores the **Authentication Protocol MS-CHAP-V2** user name. Microsoft IAS RADIUS accepts only a valid user name (dotNet user) for the Roaming Identity. For all other authentication servers, the Roaming Identity is optional. Therefore, it is recommended to use the desired realm (for example, anonymous@myrealm) for the Roaming Identity rather than a true identity.

Step 3 of 3: EAP-FAST Server

Authenticated-TLS-Server Provisioning Mode is supported using a trusted CA certificate, a self-signed server certificate, or server public keys and GTC as the inner EAP method.

1. Select one of the following credential retrieval methods: Validate Server Certificate or Specify Server or Certificate Name.
2. Click **OK** to close the security settings.

EAP-FAST User Settings

NOTE: If an Administrator Package to be exported to a user's computer does not include the Enable CCXv4 Administrator Tool Application Setting, only EAP-FAST User Settings will be available for configuration.

To set up a client with EAP-FAST authentication:

1. Click **Profiles** on the WiFi connection utility main window. Or if you are acting as the administrator, open the Administrator Tool.
2. On the Profile page, click **Add** to open the Create WiFi Profile General Settings.
3. **WiFi Network Name (SSID)**: Enter the network identifier.
4. **Profile Name**: Enter a descriptive profile name.
5. **Operating Mode**: Click **Network (Infrastructure)**. (This parameter is set to Infrastructure if you are using the Administrator Tool.)
6. **Administrator Profile Type**: Select Persistent or Pre-logon/Common. (This step applies only if you are using the Administrator Tool.)
7. Click **Next** to open the **Security Settings**.
8. Click **Enterprise Security**.
9. **Network Authentication**: Select **WPA-Enterprise** or **WPA2-Enterprise**.
10. **Data Encryption**: Select one of the following:
    - **TKIP** provides per-packet key mixing, a message integrity check and a rekeying mechanism.
    - **AES-CCMP** (Advanced Encryption Standard - Counter CBC-MAC Protocol) is used as the data encryption method whenever strong data protection is important. AES-CCMP is recommended.
11. **Enable 802.1X**: Selected.
12. **Authentication Type**: Select **EAP-FAST** to be used with this connection.
13. Click Cisco Options to select **Allow Fast Roaming (CCKM)**, which enables the client WiFi adapter for fast secure roaming.

Step 1 of 3 EAP-FAST Provisioning (User Settings)

EAP-FAST uses a PAC key to protect the user credentials that are exchanged. All EAP-FAST authenticators are identified by an authority identity (A-ID). The local authenticator sends its A-ID to an authenticating client, and the client checks its database for a matching A-ID. If the client does not recognize the A-ID, it requests a new PAC.

NOTE: If the provisioned Protected Access Credential (PAC) is valid, the WiFi connection utility does not prompt the user for acceptance of the PAC. If the PAC is invalid, the WiFi connection utility fails the provisioning automatically. A status message is displayed in the Wireless Event Viewer that an administrator can review on the user's computer.

1. Leave unchecked **Disable EAP-FAST Enhancements (CCXv4)**.
2. **Allow authenticated provisioning** and **Allow unauthenticated provisioning** are both checked.
3. **Default Server**: None selected is the default. Click **Select Server** to select a PAC from the default PAC authority server. The Protected Access Credentials selection page opens.

   NOTE: Server groups are only listed if you have installed an Administrator Package that contains EAP-FAST Authority ID (A-ID) Group settings.

   PAC distribution can also be completed manually (out-of-band). Manual provisioning lets you create a PAC for a user on an ACS server and then import it into a user's computer. A PAC file can be protected with a password, which the user needs to enter during a PAC import.

4. To import a PAC:
   a. Click **Import** to import a PAC from the PAC server.
   b. Click **Open**.
   c. Enter the PAC password (optional).
   d. Click **OK** to close this page. The selected PAC is used for this wireless profile.
5. Click **Next**.
6. If this is not a Pre-logon/Common profile, then click **Next** and jump to Step 3 of 3: EAP-FAST Server.
7. If this is a Pre-logon/Common profile, or if you are not using the Administrator Tool to create this profile, proceed to the next step.

Step 2 of 3: EAP-FAST Additional Information

1. Authentication Protocol: Select MS-CHAP-V2 or GTC
2. User Credentials: Select Use Windows Logon or Use the following.
3. If you selected **Use the following**, then enter the User Name, Domain, Password, and Confirm Password.
4. Enter the Roaming Identity: %DOMAIN%\%USERNAME
5. Click Next.

Step 3 of 3: EAP-FAST Server

1. Click **Validate Certificate** if desired and select the Certificate Issuer from the drop down menu. The default selection is Any Trusted CA.
2. If desired, click **Specify Server or Certificate Name** and enter the name. Then click **Server Name must match the specified entry exactly** or **Domain name must end with the specified entry**.
3. Click **OK**.

Back to Top

Back to Contents

Back to Contents

General Troubleshooting

Basic Troubleshooting

Problem or Symptom	Possible Solution
The wireless network card cannot connect to the access point.	Ensure that your access point is turned on, and that you have a profile for the wireless network. The security settings in your profile must match your access point's settings. Ensure that 802.1X is disabled on both your access point and your wireless card.
The wireless card drops connection occasionally.	1. Move closer to the access point. 2. Power cycle access point. 3. Update access point firmware from access point vendor support site. 4. Update the wireless LAN driver.

Your wireless connection is slower than expected.	1. Move closer to the access point. 2. Power cycle access point. 3. Update access point firmware from access point vendor support site. 4. Update the wireless LAN driver.
The name of my wireless network is not displayed in the list of available networks.	Ensure that your access point is functioning correctly. Check the SSID (network name) of the wireless network and ensure that the access point is set to broadcast the SSID.
For XP users: The computers seem to be connected to the network, but printers and/or file shares do not appear in **My Computer** or in **My Network Places**.	Verify that File and Printer Sharing is enabled on all the computers on your network. 1. Click **Start**. 2. Click **Control Panel**. 3. Click **Switch to Classic View**, if available in the left pane. 4. Double-click **Network Connections**. 5. Right-click **Wireless Network Connection**. 6. Click **Properties**. 7. Click the **General** tab. 8. Under **This connection uses the following items**, verify that the **File and Printer Sharing for Microsoft Networks** is selected. 9. If cleared, click to select **File and Printer Sharing for Microsoft Networks**. 10. If this item is not present, perform the following steps: • Click **Install**.

	- Select **Service** - Click **Add**. - Select **File and Printer Sharing for Microsoft Networks**. - Click **OK** 11. Close **OK** to close Wireless Network Connection Properties. 12. Close Network Connections.
For Vista users: The computers seem to be connected to the network, but printers and/or file shares do not appear in **Computer**.	Verify that File and Printer Sharing are enabled in the Network and Sharing Center. 1. Click **Start**. 2. Click **Control Panel**. 3. Click **Network and Internet**. 4. Under Network and Sharing Center, click **View network computers and devices**. 5. If no resources are displayed, network discovery and file sharing may be turned off. This is indicated by a message by the top of the window: **Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to change...** Click this message. 6. Click **Turn on network discovery and file sharing**. The instructions will guide you through the process.

Data transfer is sometimes very slow.	Microwave ovens, some baby monitors, cordless game controllers, and some cordless phones operate at the same radio frequency as the installed wireless card. When these devices are in use, they interfere with the wireless network. For optimum performance, keep wirelessly-connected computers at least 20 feet away from devices that operate at a frequency of 2.4 GHz.
Data transfer is always very slow.	Some homes and most offices are steel-framed structures. The steel in such buildings may interfere with your network's radio signals, thus causing a slowdown in the data transmission rate. Try moving your computer to different locations in the building to see if performance improves.
Computers are not communicating with the network.	Verify that all of the wireless network properties settings are correct. • Make sure that your computer is receiving a good signal from the access point or router. • Verify with the network administrator that installed the wireless card in your portable computer is compatible with the IEEE 802.11 WLAN standard under which the wireless network is operating. • You may need to disable or uninstall firewall software to connect. • If your network uses access points or routers, check all cables and make sure the power LED on the front of the access point or router is green.
I cannot connect to any wireless network.	Radio may be disabled. See: Turn on/Turn off Radio for more information.
Intel(R) PROSet/Wireless WiFi software asks me for a key when I try to connect to a wireless network.	Network has security enabled. See Security Overview for more information.
No WiFi networks are displayed in the list of available networks.	Computer is too far from wireless network or there are no WiFi networks in the area.

How do I configure roaming identity for multiple users?	**Configure Roaming Identity to support multiple users:** If you use a Pre-logon/Common profile that requires the roaming identity to be based on the Windows logon credentials, the creator of the profile can add a roaming identity that uses %username% and %domain%. The roaming identity is parsed and the appropriate log on information is substituted for the keywords. This allows maximum flexibility in configuring the roaming identity while allowing multiple users to share the profile. Please see your authentication server user guide for directions about how to format a suitable roaming identity. Possible formats are: %domain%\%username% %username%@%domain% %username%@%domain%.com %username%@mynetwork.com If Roaming Identity is cleared, %domain%\%username% is the default. **NOTE**: **Credentials**: This user name and domain must match the user name that is set in the authentication server by the administrator prior to client authentication. The user name is case-sensitive. This name specifies the identity supplied to the authenticator by the authentication protocol operating over the TLS tunnel. This user identity is securely transmitted to the server only after an encrypted channel has been verified and established.

Back to Top

Back to Contents

Back to Contents

Intel(R) Wireless Troubleshooter (Tools menu)

The Intel(R) Wireless Troubleshooter is an application that can help you resolve wireless network connection issues. When a connection issue is detected, a desktop *alert notification* appears at the bottom right corner of your desktop. Once you click the desktop alert, a diagnostic message displays the recommended steps to resolve the connection problem. For example, if a connection problem occurred because of an invalid password, the Profile Manager application is launched when you click a displayed hyperlink, letting you enter the correct password.

From the Intel(R) Wireless Troubleshooter you can enable or disable the alert notifications. The Intel(R) Wireless Troubleshooter is only supported under Microsoft Windows XP*.

Intel(R) Wireless Troubleshooter Window

The Intel(R) Wireless Troubleshooter contains two panes. The left pane displays a list of available tools. The right pane displays the current connection issue and is divided into two sections: the error message and the recommended action. The recommended action contains descriptions about available utilities and helps to resolve the associated connection issue. If you click on a help link, the help text is displayed in a window. If you click on the associated issue resolution link, a program is launched to resolve the connection issue.

Name	Description	
Menu Options	**File**	**Wireless Event Viewer**: Launches Wireless Event Viewer. Also selectable in the left pane.
		Disable Notification/Enable Notification: Select to disable or enable alert notifications. Also selectable in the left pane.
		Exit: Click to exit the Intel(R) Wireless Troubleshooter application.

	View	**History**: Displays or removes the History data on the right panel of the Intel(R) Wireless Troubleshooter.
	Tools	**Manual Diagnostics Tool**: Run diagnostic test to verify the functionality of your WiFi adapter. See Manual Diagnostics Tool for more information.
	Help	**Intel(R) Wireless Troubleshooter Help**: Displays online help for the Intel(R) Wireless Troubleshooter.
		About: Displays version information for the Intel(R) Wireless Troubleshooter.
Available Help	The date, time and error message: • Description of error. • Link to resolve error (if available). See Resolve Errors next. • Link to recommended steps to resolve error.	
History	Maintains a list of the last five alerts. The alerts are listed chronologically, with the most recent alert at the top of the list.	

How to Open Use Intel(R) Wireless Troubleshooter

Open the Intel(R) PROSet/Wireless WiFi Connection Utility. At the Tools menu, click **Intel (R) Wireless WiFi Troubleshooter**.

Resolve Errors

Use the following recommendations to resolve detected network connection issues.

Did not receive an IP address
The ad hoc network is idle and no peers have joined the network
The ad hoc network is idle and all peers have left the network
You are connected to a network with default network name (SSID). The network or the access point may not be configured with security
You are connected to a network that is not configured with security and there are shared folders detected in your system
The wireless network adapter in the system is disabled
No wireless network adapter was detected in the system
No wireless network adapter driver was installed
Corrupted wireless network adapter driver

Adapter Driver is not loaded
Disconnection from an access point

If you are an advanced user or administrator, use these error messages to diagnose problems within your wireless network profiles.

The application failed to start
No certificate found
Authentication failed due to invalid user name
Authentication failed due to invalid user credentials
Authentication failed due to an invalid user certificate
Your certificate will expire soon
Authentication failed due to invalid server identity
Authentication failed due to invalid server credentials
Authentication failed due to an invalid server certificate
Authentication failed because the AAA server is unavailable
The AAA server rejected the EAP method
Incorrect PIN for retrieving certificate
Error occurred because the GSM adapter was unexpectedly removed
Smart Card was unexpectedly removed
Authentication failed because timer expired
An administrator profile failed to authenticate
Administrator profile failed to authenticate due to an invalid certificate
Administrator profile did not receive an IP address

Did not receive an IP address

The WiFi adapter failed to get a valid IP address. The wireless security password or encryption key does not match the one used by the access point. Other causes are: the wireless network requires a static IP address; there is a problem with the DHCP server; or, a general network problem.

To clear this message:

- Reenter the wireless security password in the network security settings. See Personal Security.
- Restart the access point, router, computer, and DSL/cable modem.
- Verify the security configuration on the access point or wireless router. For assistance, contact your access point or router manufacturer.
- Contact your network administrator for help to set up your wireless connection.

The ad hoc network is idle and no peers have joined the network

If you create an ad hoc network and no peers join that ad hoc network for two minutes, this alert notifies you that the ad hoc network is idle.

This alert notification is enabled or disabled in the Application Settings.

To clear this message:

1. From the Tools menu, click **Application Settings**.
2. Scroll down to locate **Device to Device (ad hoc) Network Notification**.
3. Clear **Notify when no peers have joined the ad hoc network**.
4. Click **OK** to save your settings and return to the WiFi connection utility main window.

The ad hoc network is idle and all peers have left the network

If you create or join an ad hoc network with other participants, this alert notifies you when any or all participants have left the ad hoc network.

This alert notification is set in the Application Settings.

To clear this message:

1. From the Tools menu, click **Application Settings**.
2. Scroll down to locate **Device to Device (ad hoc) Network Notification**.
3. Clear **Notify when all peers leave the ad hoc network**.
4. Click **OK** to save your settings and return to the WiFi connection utility main window.

You are connected to a network with default network name (SSID). The network or the access point may not be configured with security

Connecting to an access point that uses a default network name (SSID) can be a security problem. This access point usually uses all the default security and management settings (for example, Open authentication, default IP address, user name, or password.) If this is a personal network, change the network name and security settings to improve the security of the network.

This alert notification is enabled or disabled in the Application Settings.

To clear this message:

1. From the Tools menu, click **Application Settings**.
2. Scroll down to locate **SSID Notification**.
3. Clear **Notify when connected to a network with the default SSID name**.
4. Click **OK** to save your settings and return to the WiFi connection utility main window.

You are connected to a network that is not configured with security and there are shared folders detected in your system

File and printer sharing enables other computers on a network to access resources on your computer. You should be cautious when you use your wireless portable computer with file and printer sharing enabled.

If you are alerted when connecting to a wireless LAN with shared folders, you can disable this notification. See Application Settings.

To clear this message and restore the network shared folders on disconnection:

1. From the Tools menu, click **Application Settings**.
2. Scroll down to locate **Shared Folder Notification**.
3. Select **Disable this notification** to maintain your current shared folder settings each time that you connect to an open, unsecured network.
4. Click **OK** to save your settings and return to the WiFi connection utility main window.

The wireless network adapter in the system is disabled

Enable the WiFi adapter.

1. Right-click **My Computer**.
2. Select **Properties**.
3. Click **Hardware**.
4. Click **Device Manager**.
5. Double-click **Network Adapters**.
6. Right-click the Intel(R) PRO/Wireless adapter that is listed.
7. Click **Enable**.
8. Click **File** > **Exit** to close the Device Manager.
9. Click **OK** to close System Properties.

No wireless network adapter was detected in the system

The system could not detect an Intel WiFi adapter in the system. The adapter may be removed or not installed.

First verify if there is a WiFi adapter listed in the Device Manager:

1. Right-click **My Computer**.
2. Select **Properties**.
3. Click **Hardware**.
4. Click **Device Manager**.
5. Double-click **Network Adapters**.

If an Intel(R) PRO/Wireless adapter is listed, update the driver from the Intel Corporation Support Web site at www.intel.com/support/. If an Intel(R) PRO/Wireless adapter is not listed, contact your computer manufacturer.

No wireless network adapter driver was detected in the system

The system could not detect an Intel WiFi adapter in the system. You may need to update the WiFi adapter driver.

First verify if there is a WiFi adapter listed in the Device Manager:

1. Right-click **My Computer**.
2. Select **Properties**.
3. Click **Hardware**.
4. Click **Device Manager**.
5. Double-click **Network Adapters**.

If the WiFi adapter is listed:

1. Go to **Start** > **Control Panel** > **Add or Remove Programs**.
2. Select Intel(R) PROSet/Wireless WiFi Software.
3. Click **Change**.
4. Select repair.
5. Click **Next**.

If these steps do not resolve the problem, download and install the latest software for the

Intel wireless adapter from the Intel Corporation Support Web site at www.intel.com/support/. If an Intel(R) PRO/Wireless adapter is not listed, contact your computer manufacturer.

Corrupted wireless network adapter driver

The system detected that the network driver is corrupted. You need to update the WiFi adapter driver.

1. Right click the Intel(R) PRO/Wireless network card that is installed in your computer.
2. Click **Update Driver**. The **Windows Welcome to the Hardware Update Wizard** is displayed.
3. At the Hardware Update Wizard screen, click **Yes, this time only.**
4. Click **Next**.
5. Click **Install the software automatically**. Or if you know where the driver is located, click **Install from a list or specified location**.

If an Intel(R) PRO/Wireless adapter is listed, update the driver from the Intel Corporation Support Web site at www.intel.com/support/. If an Intel(R) PRO/Wireless adapter is not listed, contact your computer manufacturer.

If you receive the message **Cannot Continue the Hardware Update Wizard**, contact the Intel Corporation Support Web site at www.intel.com/support/.

Adapter Driver is not loaded

The system detected that the WiFi adapter driver is not loaded. You need to install/update the WiFi adapter driver.

1. Right click the Intel(R) PRO/Wireless network card that is installed in your computer.
2. Click **Update Driver**. The **Windows Welcome to the Hardware Update Wizard** is displayed.
3. At the Hardware Update Wizard screen, click **Yes, this time only.**
4. Click **Next**.
5. Click **Install the software automatically**. Or if you know where the driver is located, click **Install from a list or specified location**.

If an Intel(R) PRO/Wireless adapter is listed, update the driver from the Intel Corporation Support Web site at www.intel.com/support/. If an Intel(R) PRO/Wireless adapter is not listed, contact your computer manufacturer.

If you receive the message **Cannot Continue the Hardware Update Wizard**, contact the Intel Corporation Support Web site at www.intel.com/support/.

Disconnection from an access point

The following error messages are displayed when the WiFi adapter is disconnected from the network access point.

Disconnect from access point due to failed association.
Disconnect from access point due to authentication failures.
Disconnect from access point due to TKIP Michael Integrity Check failure.
Disconnect from access point due to Class 2 frame non-authentication failure.
Disconnect from access point due to Class 3 frame non-association failure.
Disconnect from access point due to re-association failure.
Disconnect from access point due to Information Element failure.
Disconnect from access point due to EAPOL-Key protocol 4-way handshake failure.
Disconnect from access point due to 802.1X authentication failure.

Recommended action:

Manually reconnect or verify network settings stored in profile then remove the access point from the Exclude list. For example, on the WiFi connection utility main window, click **Profiles** to open the Profiles list. Select the profile and click **Connect**.

The application failed to start

The application that you specified to start when this profile connected, could not be found. Verify the path and file name in the Profile Wizard Advanced Settings.

To verify the path and file name:

1. From the WiFi connection utility main window, click **Profiles**.
2. Select the Profile.
3. Click Properties.
4. Click Advanced.
5. Click **Application Auto Launch**.
6. Click **Enable Application Auto Launch**. Verify that the file name and file location path are correct.
7. Click **OK** to close the Advanced Settings.
8. Click **OK** to close the General Settings and return to the Profiles list.

No certificate found

This error may occur if a machine certificate or a user certificate was not found in the relevant certificate store. To resolve, perform the following steps:

1. Verify that a valid machine or user certificate is present in the machine or user certificate store, depending on the type of profile you are using.
2. If a valid certificate is not present in the store, request a valid machine or user certificate from the domain's Certificate Authority. Note that the computer needs to be joined to a domain in order to be eligible to get a machine certificate from the domain's Certificate Authority.
3. Contact your Administrator for assistance.

Authentication failed due to invalid user name: Reenter user name

This authentication error can be caused by an invalid user name when using TTLS, PEAP, LEAP, EAP-SIM, or EAP-AKA profiles.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
2. Click **Properties**.
3. Click **Next**.
4. Select the appropriate 802.1X Authentication Type.
    - For TTLS and PEAP profiles: Select **Use the following** for User Credentials.
        - Verify the User Name information.
        - If **Use Windows logon** or **Prompt each time I connect** is selected, verify that the correct user credentials information is used when you connect to the wireless network. **NOTE**: This option is only available if you have the Single Sign On Pre-logon Connect component installed.
    - For LEAP profiles: Select **Use the following user name and password** and verify the user name information. If **Use Windows logon user name and password** or **Prompt for user name and password** is selected, make sure that the correct user credentials information is used when you connect to the wireless network.
    - For EAP-SIM or EAP-AKA authentication type: Verify that the correct user name is being used under **Specify user name** (identity).
5. To save the settings, click **OK**.

Authentication failed due to invalid user credentials: Reenter credentials

This authentication error can be caused by invalid user credentials when using TTLS, PEAP, or LEAP profiles.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
2. Click **Properties** to open the General Settings.
3. Click **Next** to open the **Security Settings**. **Enterprise Security** is selected.
4. The 802.1X Authentication Type should be selected.
   - For TTLS and PEAP profiles:
     - if you selected **Use the following** for User Credentials, verify that the User Name, Domain, and Password are correct.
     - if you selected **Use the Windows logon** or **Prompt each time I connect**, verify that the correct user credentials information is used when you connect to the wireless network.
   - For LEAP profiles:
     - if you selected **Use the following user name and password**, verify that the User Name, Domain, and Password are correct.
     - if you selected **Use the Windows logon user name and password** or **Prompt for the user name and password**, then verify that the correct user credentials information is used when you connect to the wireless network.
5. Click **OK** to save the settings.

Authentication failed due to an invalid user certificate: Select another certificate

This authentication error can be caused by an invalid user certificate.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
2. Click **Properties** to open the General Settings.
3. Click **Next** to open the **Security Settings**. **Enterprise Security** is selected.
4. Select the appropriate Authentication Type.
5. For TLS User: You can select to **Use the certificate issued to this computer**. Or you can click **Use a user certificate on this computer**. Then click **Select** and choose another user certificate from the list of installed certificates.
6. Click **OK**.

7. Click **OK** to save the settings.

NOTE: Certificates: The specified identity should match who the certificate is issued to and should be registered on the authentication server (for example, RADIUS server) that is used by the authenticator. Your certificate must be valid with respect to the authentication server. This requirement depends on the authentication server and generally means that the authentication server must know the issuer of your certificate as a Certificate Authority. You should be logged in with the same user name you used when the certificate was installed.

Your certificate will expire soon

This message applies to Windows XP* users only. This certificate you are using in your profile will expire soon. This message does not imply connection failure, but is instead a warning intended to help you avoid connection failure in the future. The time left from when this message is first displayed, until the certificate expires, is set by the Administrator. Use the following steps to resolve this error:

1. In the Intel® Wireless Troubleshooter window, click on the link to update your certificate.

If you are not able to obtain a new certificate, contact your Administrator.

Administrator profile failed to authenticate due to an invalid certificate

This message applies to Windows XP* profiles only. This administrator profile failed to authenticate due to an invalid certificate. This error can apply to machine certificates, user certificates, and smart cards. This error may occur for one of the following reasons:

- The certificate is expired.
- The certificate was not found in the certificate store.
- The certificate is for an invalid user.
- The certificate is in the Certificate Revocation List.

The resolution of this error varies, based on the cause. To resolve this error, apply a valid certificate.

Authentication failed due to invalid server identity: Reenter server

name

This authentication error can be caused by invalid server identity information.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
2. Click **Properties** to open the General Settings.
3. Click **Next** to open the **Security Settings**. **Enterprise Security** is selected.
4. Click **Next**.
5. On this screen, if you have selected Validate Server Certificate, then under the Certificate Issuer drop down menu, be sure you have selected the correct issuer. Or if you have selected to Specify Server or Certificate Name, be sure that a valid server of certificate name is entered. Or if you have selected **Any trusted CA**, be sure that the CA certificate is installed in the Trusted Root CA store.
6. Click **OK** to save the settings.

Authentication failed due to invalid server credentials: Reenter server credentials

This authentication error can be caused by an invalid server (domain) credential.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
2. Click **Properties** to open the General Settings.
3. Click **Next** to open the **Security Settings**. **Enterprise Security** is selected.
4. Select the appropriate 802.1X Authentication Type.
    - For TTLS, PEAP and EAP-FAST profiles: Select **Use the following** for User Credentials.
        - Verify the Domain information.
        - If **Use Windows logon user name** or **password or Prompt for the user name and password** is selected, verify that the correct **domain credentials** information is used when you connect to the wireless network. **NOTE**: This option is only available if you have the Single Sign On Pre-logon Connect component installed.
    - For LEAP profiles: Select **Use the following user name and password** and verify the domain is correct. If **Prompt for the user name and password** is selected, verify that the correct domain and password information is entered when you connect to the wireless network. (Must match what appears on the Security settings window.)
5. To save the settings, click **OK**.

Authentication failed due to an invalid server certificate: Select another certificate

This authentication error can be caused by an invalid server certificate.

Use the following steps to resolve this error:

1. Select the appropriate profile from the profiles list.
2. Click **Properties**.
3. Click **Next** to open the **Security Settings**. **Enterprise Security** is selected.
4. Select the appropriate 802.1X Authentication Type.
   - For TTLS and PEAP profiles: Verify that the correct Authentication Type is selected from the list. Click **Next to** select another certificate from the list of installed certificates or specify another server or certificate name. Click **OK**.
   - For TLS profiles: Click **Select** and choose another certificate from the list of installed certificates and click **OK**.

5. To save the settings, click **OK**.

NOTE Certificates: The specified identity should match who the certificate is issued to and should be registered on the authentication server (for example, RADIUS server) that is used by the authenticator. Your certificate must be valid with respect to the authentication server. This requirement depends on the authentication server and generally means that the authentication server must know the issuer of your certificate as a Certificate Authority. You should be logged in with the same user name you used when the certificate was installed.

Authentication failed because the AAA server is unavailable

The WiFi adapter is associated to the access point, but the 802.1X authentication cannot be completed because of a response from the authentication server.

Use the following steps to resolve this error:

1. Select the profile
2. Click **Connect** and attempt to associate with the network and authenticate with the server.

The AAA Server rejected the EAP method

This error occurs when the AAA Server does not accept the configured authentication.

Use the following steps to resolve this error:

1. Double-click the Taskbar icon to open the WiFi connection utility.
2. Click **Profiles** on the WiFi connection utility main window.
3. Select the associated or last-used profile from the Profiles list.
4. Click **Properties** to open the General Settings.
5. Click **Next** to open the **Security Settings**.
6. Verify that **Enable 802.1X** is selected.
7. Verify that the correct authentication type is selected.
8. Enter the required security information.
9. Click **OK**. The profile is now reapplied. The WiFi connection utility attempts to connect to the wireless network.

Incorrect PIN for retrieving certificate: Reenter PIN

The certificate retrieval failed because of an incorrect PIN.

Recommended action: Enter the correct PIN.

Error occurred because the GSM adapter was unexpectedly removed

This error occurs when the GSM adapter is not fully inserted or is unexpectedly removed from the mobile station.

Use the following steps to resolve this error:

1. Reinsert the GSM adapter.
2. Double-click the **Intel PROSet/Wireless WiFi Software** icon at the bottom right of the screen.
3. Select the associated or last-used profile from the profiles list.
4. Click **Connect**. The profile is now re-applied. The WiFi connection utility attempts to connect to the wireless network.

Smart Card was unexpectedly removed

This error occurred because the Smart Card was unexpectedly removed.

Use the following steps to resolve this error:

1. Insert the Smart Card.
2. Select the 802.1X EAP-SIM authentication profile.
3. Click **Connect** to try to associate with the network.

Authentication failed because timer expired

Authentication failed because the authentication timer expired while this mobile station was authenticating. A Rogue access point or a problem with the RADIUS server could have been the reason for the problem.

Recommended action:

- If a rogue access point is suspected, consider adding this access point to the excluded access point list to prevent the WiFi adapter from connecting to this access point in the future.
- If a rogue access point is not suspected, click the profile in the Profiles list. Click **Connect** to associate with the network and attempt to authenticate with the server.

An administrator profile failed to authenticate

This error occurs when the credentials in the profile are not accepted by the authenticator (for example, an access point or AAA server). Please contact your Administrator to resolve this problem.

Administrator profile did not receive an IP address

The WiFi adapter failed to get a valid IP address. The wireless security password or encryption key does not match the one used by the access point. Other causes are: the wireless network requires a static IP address; there is a problem with the DHCP server; or, a general network problem.

To clear this message, contact your network administrator to help set up your wireless connection.

Back to Top

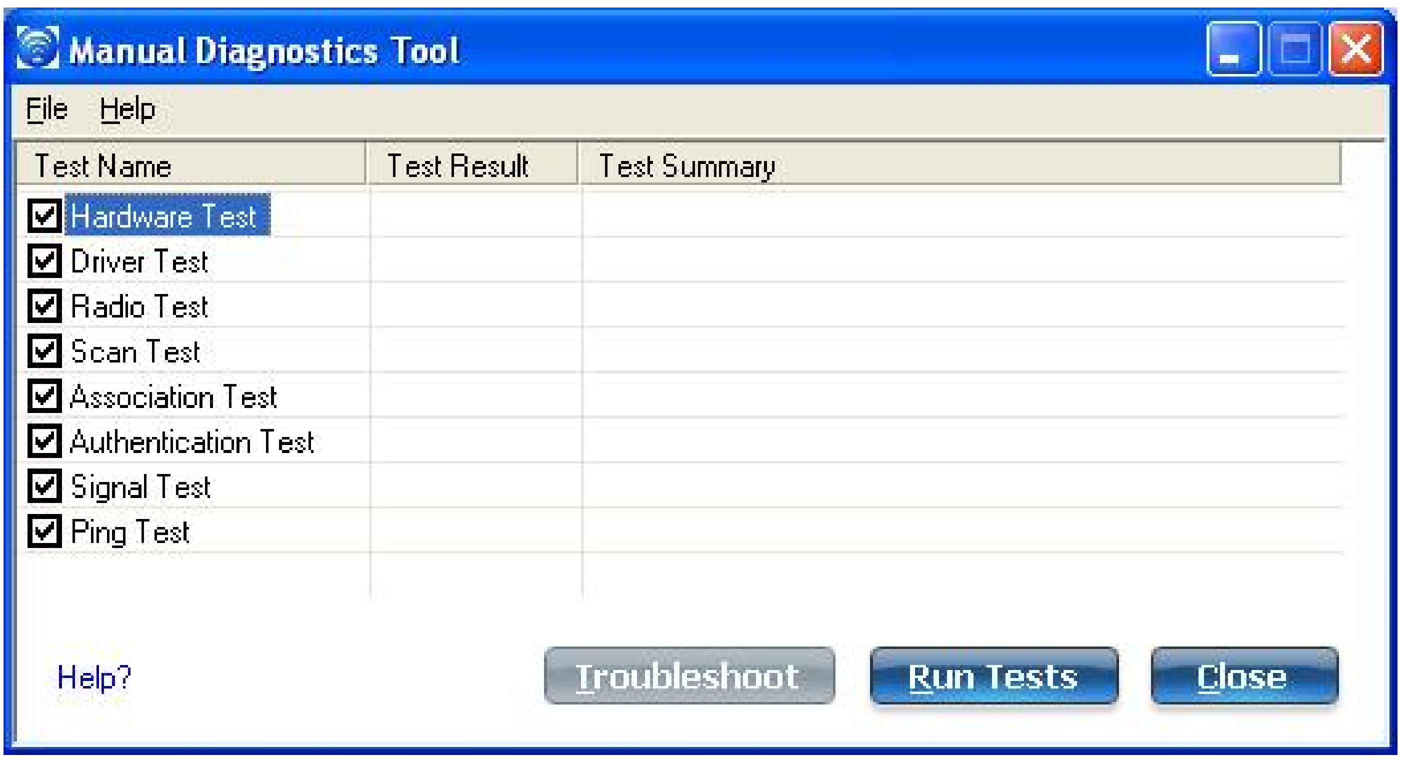
Back to Contents

Back to Contents

Manual Diagnostics Tool

The Manual Diagnostics Tool lets you run a set of diagnostics tests that verify the functionality of your WiFi adapter. There are two levels of diagnostics details represented in this tool: *user level* and *technical support level*. At the user level, the tool only shows a short description of the different diagnostics steps that are being taken and only shows a pass or fail indication for each step.

The technical support level includes the creation of a log file which contains detailed information on all the executed tests. This log file can be saved to a text file and emailed to a technical support department to troubleshoot connection problems.



Using the Manual Diagnostics Tool

To open the Manual Diagnostics tool:

- For computers running Windows XP*, first open the Intel(R) PROSet/Wireless WiFi Connection Utility. Then under the Tools menu, click **Manual Diagnostics tool**.

- For computers running Windows Vista*, click **Start** > **All Programs** > **Intel PROSet Wireless > WiFi Manual Diagnostics**.

To set the log file location:

1. Inside the Manual Diagnostics tool, click **File**.
2. Click **Settings**. The log file named WirelessDiagLog.csv contains the results of the tests. It is saved as a text file and can be used to troubleshoot network connectivity issues.
3. Click **Browse** to specify where you want the log file to be saved.
4. Click **OK** to apply your changes and return to the Manual Diagnostics Tool. The next time you run the tests, the log file will be save to your specified location.

To run the tests:

1. Click the check box next to each test to select the test to run.
2. Click **Run Tests** to run the selected tests. The test results will be saved to a file named WirelessDiagLog.csv.
3. Click **Close** to close the Manual Diagnostics Tool.

Available Tests

Name	Description
Hardware Test	The test passes if the WiFi adapter is present and accessible. The test fails if the adapter is not present or present but disabled. The test summary displays whether the wireless hardware is enabled or disabled. **Troubleshooting** • Verify that your adapter is listed under **Network adapters** in the Device Manager. • If the adapter is not listed, right-click **Network adapters** and select **Scan for hardware changes**. You can also reboot your system. • Verify that your adapter is enabled in the Device Manager. When the adapter is disabled, a red X is displayed on the device. Right-click the adapter and select **Enable** from the menu. • When the adapter displays a yellow exclamation point, right-click the adapter and reinstall the driver. • Contact your computer manufacturer for other troubleshooting options.

Driver Test	The test summary displays the Intel(R) PRO/Wireless Network Connection driver supported by the WiFi adapter. The test verifies if the driver binary version is compatible with the installed version of the WiFi connection utility. The test fails if the driver binary is not found or if the driver version does not match the WiFi connection utility software version (for example, version 11.1.x.x and driver version 9.0.x.x, 9.1.x.x, or 11.1.x.x). **Troubleshooting** • Reinstall the drivers using the WiFi connection utility.
Radio Test	The test summary displays Radio On or Radio Off. The test queries the current radio state. If the radio is switched on, the test passes. If the radio is off, the test fails. **Troubleshooting** Verify that your WiFi adapter's radio is on. There are two methods to turn the radio on and off: • The hardware switch • The **WiFi On / WiFi Off** button in the WiFi connection utility main window. See Turn On or Off the Wireless Radio for more information.
Scan Test	The test queries the WiFi networks within range of your WiFi adapter. The test passes if networks can be seen in the scan list. The Test Summary displays the number of networks available to connect to. **Troubleshooting** • Verify that you are within range of an access point. • Switch the wireless radio to off and back to on. • Verify that the wireless band setting matches the access point band setting. • Switch the access point to off and back to on.

Association Test	The test summary displays Associated or Not Associated. Association is the establishment and maintenance of the wireless link between devices. When security is enabled, the devices only exchange security credentials. The test checks for wireless connectivity. The test passes if the client is associated successfully. **Troubleshooting** • When the access point signal strength is low, use the signal test listed below. • Verify that a profile has been created. If created: ○ Verify that the profile SSID matches the access point Network Name (SSID). ○ Remove the profile and create a new profile. • Verify that your wireless network is not included in the Exclude (profiles) List. • Verify that the MAC address has not been excluded in the access point.
Authentication Test	Describes the process after association, during which the identity of the wireless device or end-user is verified and then allowed network access. The test queries for authentication state information, including all Cisco Compatible Extensions and security-related information. The test passes if the client is authenticated successfully. The test fails if the WEP key or other credentials are not authenticated. The Test Summary displays whether authentication is required for the network connection. **Troubleshooting** • Edit your profile to ensure the correct credentials have been used for the WEP key, PSK, password or certificates. • Remove the existing profile and create a new profile.

Signal Test	The test summary displays the signal quality. If the signal quality is low, use the **Troubleshoot** button to diagnose and fix the problem. **Troubleshooting** • Move your computer 10 to 20 feet from the wireless access point or router. • Reduce interference by moving away from appliances (microwaves, cell phones or 2.4 GHz phones) or access points using the same channel. • Try increasing the transmission power of the access point.
Ping Test	The test verifies whether the WiFi adapter successfully sent messages to and received replies from the access point IP address, default gateway, DHCP server (if enabled) and DNS servers. The test summary displays whether replies from these entities were received. Example: Response: AP, default gateway. No Response: DHCP server **NOTE**: If the ping tests to this access point and default gateway are successful but the ping test to the DNS server fails this is not a wireless network issue but a general network issue. **Troubleshooting** • Disable the security firewall and try the ping test again. • Contact the access point manufacturer to troubleshoot your home network. • Enterprise users should contact their network administrator.
Troubleshoot	Diagnose and fix problems displayed by each of the tests. The **Troubleshoot** button becomes active if the test fails.
Run Tests	Executes the tests that you have selected.
Close	Closes the page.
Help?	Provides help information for this page.

[Back to Top]

[Back to Contents]

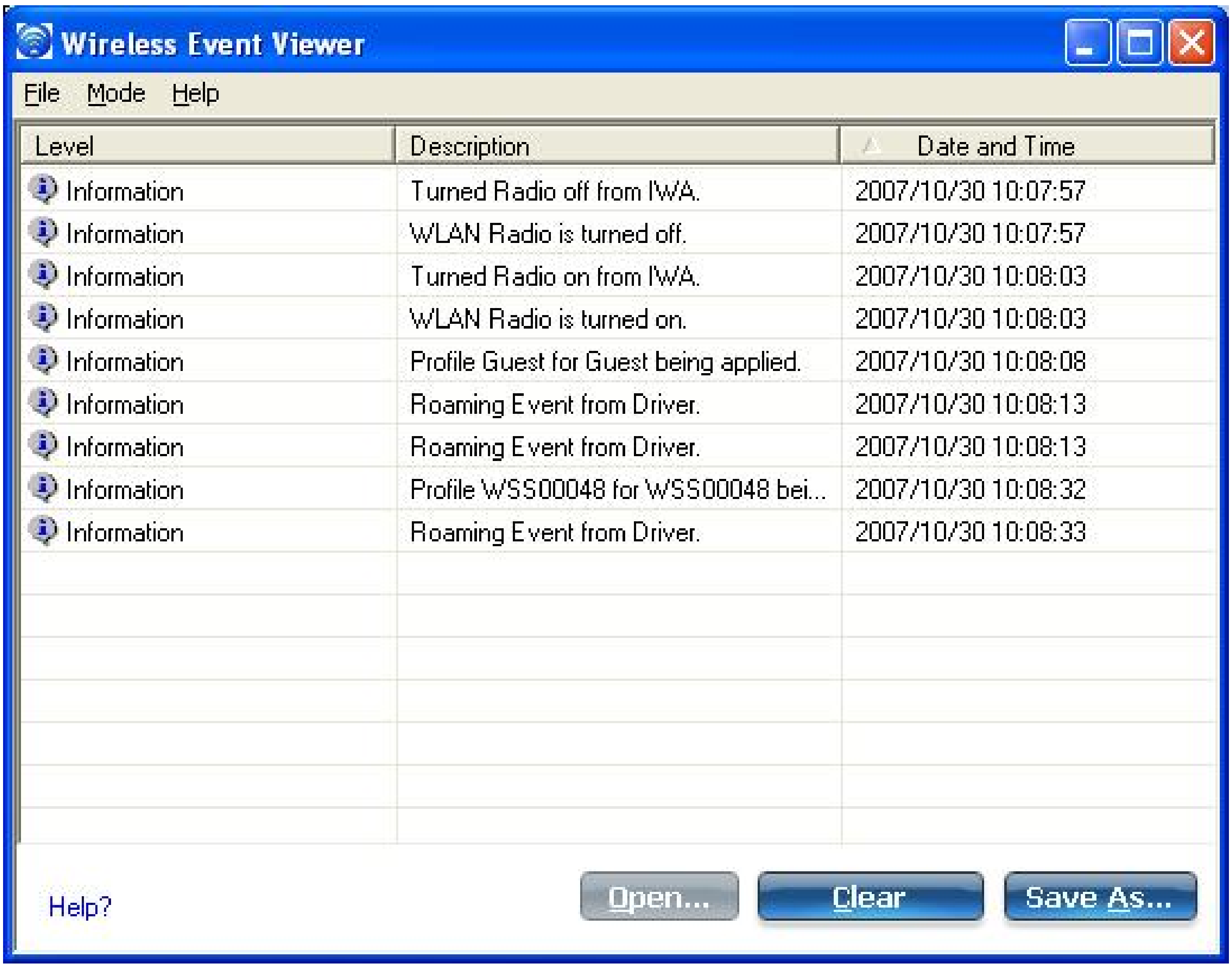
Back to Contents

Wireless Event Viewer

The Wireless Event Viewer program displays a list of error log records. You can save all available log records to a binary format file for sending to customer support.

To launch Wireless Event Viewer:

1. At the Tools menu, click Intel® Wireless Troubleshooter.
2. Click **Wireless Event Viewer**.



Wireless Event Viewer Description

Name	Description
File	**Settings**: To change the storage location of the log file. 1. Click **File > Settings** to open the **Wireless Event Viewer Settings**. 2. **Specify the default folder for saved log files**: The default location is **My Documents**. Click **Browse** to locate a new folder location. 3. **File Name**: The file name is the default machine name. 4. **Maximum file size (KB)**: Enter the size of the file in kilobytes (KB). 5. Click **OK** to close and apply the new changes. Click **Cancel** to close without applying any changes. If you want the log file copied to an archive site after a specific number of days: 1. Click **Copy the log file to another location**. 2. **Destination folder**: Enter where to store the files or click **Browse** to select a folder location. 3. **Frequency (days)**: Select how often you want the files moved to the destination folder. 4. Click **OK** to close and apply the new changes. Click **Cancel** to close without applying any changes. **Exit**: Click to exit Wireless Event Viewer and return to the Intel(R) Wireless Troubleshooter. **NOTE**: An administrator can use the Administrator Tool, Application Settings, Wireless Event Viewer Settings to set the default log file location.
Mode	Select to view current or previously saved event records: • **Real time Event Viewing**: Select this to view error events as they occur in real time. • **Log File Viewing**: Select this to open an error log file that has been previously saved, or to save the current error event log to a file.
Help?	Provides help information for this page. **About**: Displays version information for the Intel(R) Wireless Troubleshooter.

Wireless Event Viewer Information	**Level**: The severity level of the connection issue is indicated by an icon. The severity levels are: • Information • Error • Warning	
	Description: Brief description of the connection issue.	
	Date and Time: Date and time of the detected connection issue. This column can be sorted in ascending or descending order. Click the column header to sort the displayed events.	
Open	Opens log files archived from previous sessions with Intel (R) Wireless Troubleshooter.	
Clear	Removes the information in the Wireless Event Viewer.	
Save As	Saves the available log. Use the suggested name or change it.	

Back to Top

Back to Contents

Back to Contents

Specifications

Intel(R) WiMAX/WiFi Link 5350 and Intel(R) WiMAX/WiFi Link 5150

WiFi / WiMAX	
Form Factor	PCI Express* Mini Card and Half-Mini Card
SKUs	Intel® WiMAX/WiFi Link 5350 - 3x3 MC Intel® WiMAX/WiFi Link 5150 - 1x2 MC/HMC
Dimensions	Mini Card: Width 2.0 in x Length 1.18 in x Height 0.18 in (50.80 mm x 30 mm x 4.5 mm) Half-Mini Card: Width 1.049 in x Length 1.18 in x Height 0.18 in (26.64 mm x 30 mm x 4.5 mm)
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066
Antenna Diversity	On-board diversity
Connector Interface	53-pin Mini Card edge connector
Voltage	3.3 V

Operating Temperature	0 to +80 degrees Celsius	
Humidity	50% to 90% non-condensing (at temperatures of 25 ºC to 35 ºC)	
WiFi		
Frequency Modulation	**5 GHz (802.11a/n)**	**2.4 GHz (802.11b/g/n)**
Frequency band	5.15 GHz - 5.85 GHz (dependent on country)	2.41-2.474 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Medium	5 GHz UNII: Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 (dependent on country)	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
IEEE 802.11n Data Rates	**Intel(R) WiFi Link 5350** 450, 405, 360, 300, 270, 243, 240, 216.7, 195, 180, 173.3, 150, 144, 135, 130, 120, 117, 115.5, 90, 86.667, 72.2, 65, 60, 57.8, 45, 43.3, 30, 28.9, 21.7, 15, 14.4, 7.2 Mbps	
	Intel(R) WiFi Link 5150 300, 270, 243, 240, 180, 150, 144, 135, 130, 120, 117, 115.5, 90, 86.667, 72.2, 65, 60, 57.8, 45, 43.3, 30, 28.9, 21.7, 15, 14.4, 7.2 Mbps	
IEEE 802.11a Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11g Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11b Data Rates	11, 5.5, 2, 1 Mbps	
WiFi General		
Operating Systems	Microsoft Windows XP* (32 and 64 bit) and Windows Vista* (32 and 64 bit)	
Wi-Fi Alliance* certification	Wi-Fi* certification for 802.11b, 802.11g, 802.11a, 802.11h, 802.11d, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WMM, WMM Power Save, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS	
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0	

WLAN Standard	IEEE 802.11g, 802.11b, 802.11a, 802.11n	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, 802.1X: EAP-SIM, LEAP, PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA	
Encryption	AES-CCMP 128-bit, WEP 128-bit and 64-bit, CKIP, TKIP	
Product Safety	UL, C-UL, CB (IEC 60590)	
WiMAX		
Frequency band	2.5-2.7 GHz (3A Profile)	
Modulation	UL - QPSK, 16 QAM DL - QPSK, 16 QAM, 64 QAM	
Wireless Medium	Duplex mode: TDD operations	Scalable OFDMA (SOFDMA): 512 and 1024 FFT
	sub-carrier permutation: PUSC	Channel bandwidths: 5 MHz and 10 MHz
WiMAX Network Release Feature set	SPWG/NWG Release 1.0 SPWG/NWG Release 1.5	
Rate Performance	10 Mbps DL and 4 Mbps UL @ peak rate (OTA performance, 10MHz channel)	
RF Transmitter Output Power	Compliance with Power class 2	
WiMAX General		
Operating Systems	Microsoft Windows XP* ,Vista*	
Standard Compliance	802.16e-2005 Corrigenda 2 (D4)	
WiMAX System Profile Feature set	Mobile WiMAX release 1, Wave II Profile 3A	
Security	Key Management Protocol (PKMv2)	
Encryption	128-bit CCMP (Counter-Mode/CBC-MAC) based on AES encryption	

Intel(R) WiFi Link 5100 and Intel(R) WiFi Link 5300

Form Factor	PCI Express* Full-Mini Card and Half-Mini Card

Dimensions	Full-Mini Card: Width 2.00 in x Length 1.18 in x Height 0.18 in (50.95 mm x 30 mm x 4.5 mm) Half-Mini Card: Width 1.049 in x Length 1.18 in x Height 0.18 in (26.64 mm x 30 mm x 4.5 mm)	
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066	
Antenna Diversity	On-board diversity	
Connector Interface	52-pin Mini Card edge connector	
Voltage	3.3 V	
Operating Temperature	0 to +80 degrees Celsius	
Humidity	50% to 95% non-condensing (at temperatures of 25 ºC to 35 ºC)	
Frequency Modulation	**5 GHz (802.11a/n)**	**2.4 GHz (802.11b/g/n)**
Frequency band	5.15 GHz - 5.85 GHz (dependent on country)	2.400 - 2.4835 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Medium	5 GHz UNII: Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 (dependent on country)	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
IEEE 802.11n Data Rates	**Intel(R) WiFi Link 5300** 450, 405, 360, 300, 270, 243, 240, 216.7, 195, 180, 173.3, 150, 144, 135, 130, 120, 117, 115.5, 90, 86.667, 72.2, 65, 60, 57.8, 45, 43.3, 30, 28.9, 21.7, 15, 14.4, 7.2 Mbps	
	Intel(R) WiFi Link 5100 300, 270, 243, 240, 180, 150, 144, 135, 130, 120, 117, 115.5, 90, 86.667, 72.2, 65, 60, 57.8, 45, 43.3, 30, 28.9, 21.7, 15, 14.4, 7.2 Mbps	
IEEE 802.11a Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11g Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11b Data Rates	11, 5.5, 2, 1 Mbps	
General		

Operating Systems	Microsoft Windows XP* (32 and 64 bit) and Windows Vista* (32 and 64 bit).
Wi-Fi Alliance* certification	Wi-Fi* certification for 802.11b, 802.11g, 802.11a, 802.11h, 802.11d, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WMM, WMM Power Save, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a, 802.11n
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, AES-CCMP 128-bit, WEP 128-bit and 64-bit; 802.1X: EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA
Product Safety	UL, C-UL, CB (IEC 60590)

Intel(R) Wireless WiFi Link 4965AGN

Form Factor	PCI Express* Mini Card
Dimensions	Width 2.00 in x Length 1.18 in x Height 0.18 in (50.95 mm x 30 mm x 4.5 mm)
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066
Antenna Diversity	On-board diversity
Connector Interface	52-pin Mini Card edge connector
Voltage	3.3 V
Operating Temperature	0 to +80 degrees Celsius

Humidity	50% to 95% non-condensing (at temperatures of 25 ºC to 35 ºC)	
Frequency Modulation	**5 GHz (802.11a/n)**	**2.4 GHz (802.11b/g/n)**
Frequency band	5.15 GHz - 5.85 GHz (dependent on country)	2.400 - 2.4835 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Medium	5 GHz UNII: Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 (dependent on country)	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
IEEE 802.11n Data Rates	**Rx**: 300, 270, 243, 240, 180 **Rx/Tx**: 150, 144, 135, 130, 120, 117, 115.5, 90, 86.667, 72.2, 65, 60, 57.8, 45, 43.3, 30, 28.9, 21.7, 15, 14.4, 7.2	
IEEE 802.11a Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11g Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11b Data Rates	11, 5.5, 2, 1 Mbps	
General		
Operating Systems	Microsoft Windows XP* (32 and 64 bit) and Windows Vista* (32 and 64 bit).	

Wi-Fi Alliance* certification	Wi-Fi* certification for 802.11b, 802.11g, 802.11a, 802.11h, 802.11d, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WMM, WMM Power Save, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a, 802.11n
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, AES-CCMP 128-bit, WEP 128-bit and 64-bit; 802.1X: EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA
Product Safety	UL, C-UL, CB (IEC 60590)

Intel(R) Wireless WiFi Link 4965AG_

This is a version of Intel Wireless WiFi 4965AGN with 8-2.11n capabilities disabled. 802.11n refers to: IEEE P802.11n / D2.0 Draft Amendment to STANDARD [FOR] Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Enhancements for Higher Throughput.

Form Factor	PCI Express Mini Card
Dimensions	Width 2.00 in x Length 1.18 in x Height 0.18 in (50.95 mm x 30 mm x 4.5 mm)
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066
Antenna Diversity	On-board diversity
Connector Interface	52-pin Mini Card edge connector
Voltage	3.3 V
Operating Temperature	0 to +80 degrees Celsius

Humidity	50% to 95% non-condensing (at temperatures of 25 ºC to 35 ºC)	
Frequency Modulation	**5 GHz (802.11a)**	**2.4 GHz (802.11b/g)**
Frequency band	5.15 GHz - 5.85 GHz (dependent on country)	2.400 - 2.4835 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Medium	5 GHz UNII: Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 (dependent on country)	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
IEEE 802.11a Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11g Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	
IEEE 802.11b Data Rates	11, 5.5, 2, 1 Mbps	
General		
Operating Systems	Microsoft Windows XP (32 and 64 bit), and Windows Vista (32 and 64 bit)	
Wi-Fi Alliance* certification	Wi-Fi* certification for 802.11b, 802.11g, 802.11a, WPA, WPA2, WMM, EAP-SIM	
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, AES-CCMP 128-bit, WEP 128-bit and 64-bit; 802.1X: EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA	
Product Safety	UL, C-UL, CB (IEC 60590)	

Intel(R) PRO/Wireless 3945ABG Network Connection

Form Factor	PCI Express Mini Card
Dimensions	Width 2.00 in x Length 1.18 in x Height 0.18 in (50.95 mm x 30 mm x 4.5 mm)
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066

Dual Diversity Antenna	On-board dual diversity switching	
Connector Interface	52-pin Mini Card edge connector	
Voltage	3.3 V	
Operating Temperature	0 to +80 degrees Celsius	
Humidity	50 to 92% non-condensing (at temperatures of 25 ºC to 55 ºC)	
Frequency Modulation	**5 GHz (802.11a)**	**2.4 GHz (802.11b/g)**
Frequency band	5.15 GHz - 5.85 GHz	2.400 - 2.4835 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Medium	5 GHz UNII: Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 non-overlapping, dependent on country	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps
General		
Operating Systems	Microsoft Windows XP and Windows Vista	
Wi-Fi Alliance* certification	Wi-Fi* certification for 802.11b, 802.11g, 802.11a, 802.11h, 802.11d, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WMM, WMM Power Save, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA	
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, AES-CCMP 128-bit, WEP 128-bit and 64-bit; 802.1X: EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA	
Product Safety	UL, C-UL, CB (IEC 60590)	

Intel(R) PRO/Wireless 3945BG Network Connection

Form Factor	PCI Express Mini Card
Dimensions	Width 2.00 in x Length 1.18 in x Height 0.18 in (50.95 mm x 30 mm x 4.5 mm)
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066
Dual Diversity Antenna	On-board dual diversity switching
Connector Interface	52-pin Mini Card edge connector
Voltage	3.3 V
Operating Temperature	0 to +80 degrees Celsius
Humidity	50 to 92% non-condensing (at temperatures of 25 ºC to 55 ºC)
Frequency Modulation	**2.4 GHz (802.11b/g)**
Frequency band	2.400 - 2.4835 GHz (dependent on country)
Modulation	CCK, DQPSK, DBPSK
Wireless Medium	2.4 GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
IEEE 802.11g Data Rates	54, 48, 36, 24, 18, 12, 9, 6, 5.5, 2, 1 Mbps
IEEE 802.11g Data Rates	11, 5.5, 2, 1 Mbps
General	
Operating Systems	Microsoft Windows XP and Windows Vista
Wi-Fi Alliance* certification	Wi-Fi* certification for 802.11b, 802.11g, WPA, WPA2, WMM, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0
WLAN Standard	IEEE 802.11g, 802.11b
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, AES-CCMP 128-bit, WEP 128-bit and 64-bit; 802.1X: EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA
Product Safety	UL, C-UL, CB (IEC 60590)

Intel(R) PRO/Wireless 2915ABG Network Connection

Form Factor	Mini PCI Type 3A	
Dimensions	Width 2.85 in x Length 1.75 in x Height 0.20 in (72.39 mm x 44.54 mm x 5.08 mm)	
Weight	0.7 oz. (12.90 g.)	
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066	
Dual Diversity Antenna	On-board dual diversity switching	
Connector Interface	124-pin SO-DIMM edge connector	
Voltage	3.3 Volt	
Operating Temperature	0 to +70 degrees Celsius	
Humidity	50 to 85% non-condensing	
Frequency Modulation	**5 GHz (802.11a)**	**2.4 GHz (802.11b/g)**
Frequency band	5.15 GHz - 5.85 GHz	2.400 - 2.472 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Medium	5 GHz UNII: Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 non-overlapping, dependent on country	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)

Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps
General		
Operating Systems	Microsoft Windows XP and Windows Vista	
Wi-Fi Alliance* certification	Wi-Fi* certification for 802.11b, 802.11g, 802.11a, WPA, WPA2, WMM, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA	
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v3.0	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, AES-CCMP 128-bit, WEP 128-bit and 64-bit. 802.1X: EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA	
Product Safety	UL, C-UL, CB (IEC 60590)	

Intel(R) PRO/Wireless 2200BG Network Connection

Form Factor	Mini PCI Type 3B
Dimensions	Width 2.34 in x Length 1.75 in x Height 0.20 in (59.45 mm x 44.45 mm x 5 mm)
Weight	0.7 oz. (12.90 g.)
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066
Dual Diversity Antenna	On-board dual diversity switching
Connector Interface	124-pin mini PCI edge connector
Voltage	3.3 V

Operating Temperature	0 to +70 degrees Celsius
Humidity	50 to 85% non-condensing
Frequency Modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK
Frequency band	2.400 - 2.472 GHz (US) 2.400 - 2.4835 GHz (Japan) 2.400 - 2.4835 GHz (Europe ETSI)
Modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK
Channels	Full 14 channel support
Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps
General	
Operating Systems	Microsoft Windows XP and Windows Vista
Wi-Fi Alliance* certification	Wi-Fi* certification for 802.11b, 802.11g, WPA, WPA2, WMM, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-AKA
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v2.0
WLAN Standard	IEEE 802.11g and 802.11b
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes
Security	WPA, LEAP, PEAP, TKIP, EAP-TLS, EAP-TTLS, AES (128-bit), WEP 128-bit and 64-bit.
Product Safety	UL, C-UL, CB (IEC 60590)

[Back to Top]

[Back to Contents]

[Trademarks and Disclaimers]

Back to Contents

Regulatory Information

Intel(R) WiMAX/WiFi Link 5350 and Intel(R) WiMAX/WiFi Link 5150 Adapters

The information in this section applies to the following products:

WiMAX and Wireless LAN Adapters

- Intel(R) WiMAX/WiFi Link 5150 (model numbers 512ANX_MMW, 512ANX_HMW)
- Intel(R) WiMAX/WiFi Link 5350 (model number 533ANX_ MMW)

NOTE: In this section, all references to "the adapter" refer equally to the Intel® WiMAX/WiFi Link 5350 and Intel® WiMAX/WiFi Link 5150 adapters.

NOTE: Due to the evolving state of regulations and standards in the wireless LAN field (IEEE 802.11 and similar standards), the information provided herein is subject to change. Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

Information for the User

Safety Notices

USA—FCC and FAA

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The adapter meets the Human Exposure limits found in OET Bulletin 65, supplement C, 2001, and ANSI/IEEE C95.1, 1992. Proper operation of this radio according to the instructions found in this manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

- Do not touch or move antenna while the unit is transmitting or receiving.
- Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; this behavior may cause damage to the radio.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited by the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

Antenna Use

- In order to comply with FCC RF exposure limits, low gain integrated antennas should be located at a minimum distance of 20 cm (8 inches) or more from the body of all persons.
- High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 30 cm (12 inches) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.

Explosive Device Proximity Warning

Warning: Do not operate a portable transmitter (such as a wireless network adapter) near unshielded blasting caps or in an explosive environment unless the adapter has been modified to be qualified for such use.

Antenna Warnings

Warning: To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended that for the adapter installed in a desktop or portable computer, the antenna for this adapter to be installed so as to provide a separation distance of at least 20 cm (8 inches) from all persons. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

Warning: Intel(R) PRO/Wireless LAN products are not designed for use with high-gain directional antennas. Use of such antennas with these products in a manner other than as described in the previous section titled, "Antenna Use" is illegal.

Use On Aircraft Caution

Caution: Regulations of the FCC and FAA prohibit airborne operation of radio-frequency wireless adapters because their signals could interfere with critical aircraft instruments.

Other Wireless Devices

Safety Notices for Other Devices in the Wireless Network: See the documentation supplied with wireless adapters or other devices in the wireless network.

Local Restrictions on 802.11a, 802.11b, 802.11g, 802.11n, and 802.16e Radio Usage

⚠ **Caution**: Due to the fact that the frequencies used by 802.11a, 802.11b, 802.11g, 802.11n, and 802.16e wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, 802.11g, 802.11n, and 802.16e products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. The device transmit power control (TPC) interface is part of the Intel(R) PROSet/Wireless WiFi Connection Utility Software. Operational restrictions for Equivalent Isotropic Radiated Power (EIRP) are provided by the system manufacturer. Any deviation from the permissible power and frequency settings for the country of use is an infringement of national law and may be punished as such.

For country-specific information, see the additional compliance information supplied with the product.

Wireless Interoperability

The adapter is designed to be interoperable with other wireless LAN products that are based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

- IEEE Std. 802.11b compliant Standard on Wireless LAN
- IEEE Std. 802.11g compliant Standard on Wireless LAN
- IEEE Std. 802.11a compliant Standard on Wireless LAN
- IEEE Std. 802.11n draft 2.0 compliant on Wireless LAN
- IEEE 802.16e-2005 Wave 2 compliant
- Wireless Fidelity certification, as defined by the Wi-Fi Alliance
- WiMAX certification as defined by the WiMAX Forum

The Intel® WiMAX/WiFi Link 5350, Intel® WiMAX/WiFi Link 5150 Adapter, and Your Health

The adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by the adapter, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The adapter operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the adapter may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:

- Using the adapter equipment on board airplanes, or
- Using the adapter equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the adapter before you turn it on.

Regulatory Information

Information for the OEMs and Integrators

The following statement must be included with all versions of this document supplied to an OEM or integrator, but should not be distributed to the end user.

- This device is intended for OEM integrators only.
- Please see the full Grant of Equipment document for other restrictions.
- This device must be operated and used with a locally approved access point.

Information To Be Supplied to the End User by the OEM or Integrator

The following regulatory and safety notices must be published in documentation supplied to the end user of the product or system incorporating an adapter in compliance with local regulations. Host system must be labeled with "Contains FCC ID: XXXXXXXX", FCC ID displayed on label.

The Intel® WiMAX/WiFi Link 5350 adapter or Intel® WiMAX/WiFi Link 5150 adapter must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel® WiMAX/WiFi Link 5350 adapter kit or Intel® WiMAX/WiFi Link 5150 adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

Local Restriction of 802.11a, 802.11b, 802.11g, and 802.11n Radio Usage

The following statement on local restrictions must be published as part of the compliance documentation for all 802.11a, 802.11b, 802.11g and 802.11n products.

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, 802.11g and 802.11n wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, 802.11g and 802.11n products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. Any deviation from permissible settings and restrictions in the country of use could be an infringement of national law and may be punished as such.

FCC Radio Frequency Interference Requirements

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. FCC requires this product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems. High power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with and /or damage this device.

- This device is intended for OEM integrators only.
- This device cannot be co-located with any other transmitter unless approved by the FCC.

USA—Federal Communications Commission (FCC)

This device complies with Part 15 of the FCC Rules. Operation of the device is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

NOTE: The radiated output power of the adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the adapter should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 20 cm between you (or any other person in the vicinity) and the antenna that is built into the computer. Details of the authorized configurations can be found at http://www.fcc.gov/oet/ea/ by entering the FCC ID number on the device.

Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If the equipment is not installed and used in accordance with the instructions, the equipment may cause harmful interference to radio communications. There is no guarantee, however, that such interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

> **NOTE**: The adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations.

Underwriters Laboratories Inc. (UL) Regulatory Warning

For use in (or with) UL Listed personal computers or compatible.

Regulatory Markings

A list of required regulatory markings can be found on the web at xxxxxxxxxx (link under construction).

Intel(R) WiFi Link 5300 and Intel(R) WiFi Link 5100 Adapters

The information in this section applies to the following products:

Quad-mode wireless LAN adapters (802.11a/802.11b/802.11g/802.11n draft 2.0)

- Intel(R) WiFi Link 5100 (model numbers 512AN_HMW, 512AN_MMW, 512AG_HMW, 512AG_MMW)
- Intel(R) WiFi Link 5300 (model numbers 533AN_HMW, 533AN_MMW)

> **NOTE**: In this section, all references to "the adapter" refer equally to the Intel(R) WiFi Link 5300 and Intel(R) WiFi Link 5100 adapters.

> **NOTE**: Due to the evolving state of regulations and standards in the wireless LAN field (IEEE 802.11 and similar standards), the information provided herein is subject to change. Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

Information for the User

Safety Notices

USA—FCC and FAA

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The adapter meets the Human Exposure limits found in OET Bulletin 65, supplement C, 2001, and ANSI/IEEE C95.1, 1992. Proper operation of this radio according to the instructions found in this manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

- Do not touch or move antenna while the unit is transmitting or receiving.
- Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; this behavior may cause damage to the radio.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited by the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).

- The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

Antenna Use

- In order to comply with FCC RF exposure limits, low gain integrated antennas should be located at a minimum distance of 20 cm (8 inches) or more from the body of all persons.
- High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 30 cm (12 inches) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.

Explosive Device Proximity Warning

Warning: Do not operate a portable transmitter (such as a wireless network device) near unshielded blasting caps or in an explosive environment unless the device has been modified to be qualified for such use.

Antenna Warnings

Warning: To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended for the adapter installed in a desktop or portable computer, that the antenna for this device be installed so as to provide a separation distance of at least 20 cm (8 inches) from all persons. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

Warning: Intel(R) PRO/Wireless LAN products are not designed for use with high-gain directional antennas. Use of such antennas with these products in a manner other than as described in the previous section titled, “Antenna Use” is illegal.

Use On Aircraft Caution

Caution: Regulations of the FCC and FAA prohibit airborne operation of radio-frequency wireless devices because their signals could interfere with critical aircraft instruments.

Other Wireless Devices

Safety Notices for Other Devices in the Wireless Network: See the documentation supplied with wireless adapters or other devices in the wireless network.

Local Restrictions on 802.11a, 802.11b, 802.11g and 802.11n Radio Usage

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, 802.11g and 802.11n wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, 802.11g and 802.11n products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. The device transmit power control (TPC) interface is part of the Intel(R) PROSet/Wireless WiFi Connection Utility Software. Operational restrictions for Equivalent Isotropic Radiated Power (EIRP) are provided by the system manufacturer. Any deviation from the permissible power and frequency settings for the country of use is an infringement of national law and may be punished as such.

For country-specific information, see the additional compliance information supplied with the product.

Wireless Interoperability

The adapter is designed to be interoperable with other wireless LAN products that are based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

- IEEE Std. 802.11b compliant Standard on Wireless LAN
- IEEE Std. 802.11g compliant Standard on Wireless LAN
- IEEE Std. 802.11a compliant Standard on Wireless LAN

- IEEE Std. 802.11n draft 2.0 compliant on Wireless LAN
- Wireless Fidelity certification, as defined by the Wi-Fi Alliance

The Intel(R) WiFi Link 5300 Adapter, Intel(R) WiFi Link 5100 Adapter, and Your Health

The adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by this device, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The adapter operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the adapter may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:

- Using the adapter equipment on board airplanes, or
- Using the adapter equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the adapter before you turn it on.

Regulatory Information

Information for the OEMs and Integrators

The following statement must be included with all versions of this document supplied to an OEM or integrator, but should not be distributed to the end user.

- This device is intended for OEM integrators only.
- Please see the full Grant of Equipment document for other restrictions.
- This device must be operated and used with a locally approved access point.

Information To Be Supplied to the End User by the OEM or Integrator

The following regulatory and safety notices must be published in documentation supplied to the end user of the product or system incorporating an Intel(R) WiFi Link 5300 adapter or Intel(R) WiFi Link 5100 adapter in compliance with local regulations. Host system must be labeled with "Contains FCC ID: XXXXXXXX", FCC ID displayed on label.

The Intel(R) WiFi Link 5300 adapter or Intel(R) WiFi Link 5100 adapter must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific approvals, see Radio Approvals. Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel(R) WiFi Link 5300 adapter kit or Intel(R) WiFi Link 5100 adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation and authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

Local Restriction of 802.11a, 802.11b, 802.11g, and 802.11n Radio Usage

The following statement on local restrictions must be published as part of the compliance documentation for all 802.11a, 802.11b, 802.11g and 802.11n products.

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, 802.11g and 802.11n wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, 802.11g and 802.11n products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. Any deviation from permissible settings and restrictions in the country of use could be an infringement of national law and may be punished as such.

FCC Radio Frequency Interference Requirements

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. FCC requires this product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems. High power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with and /or damage this device.

- This device is intended for OEM integrators only.
- This device cannot be co-located with any other transmitter unless approved by the FCC.

USA—Federal Communications Commission (FCC)

This device complies with Part 15 of the FCC Rules. Operation of the device is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

NOTE: The radiated output power of the adapter is far below the FCC radio frequency exposure limits. Nevertheless, the adapter should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 20 cm between you (or any other person in the vicinity) and the antenna that is built into the computer. Details of the authorized configurations can be found at http://www.fcc.gov/oet/ea/ by entering the FCC ID number on the device.

Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If the equipment is not installed and used in accordance with the instructions, the equipment may cause harmful interference to radio communications. There is no guarantee, however, that such interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

NOTE: The adapter must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations.

Underwriters Laboratories Inc. (UL) Regulatory Warning

For use in (or with) UL Listed personal computers or compatible.

Brazil

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Canada—Industry Canada (IC)

This device complies with RSS210 of Industry Canada.

Caution: When using IEEE 802.11a wireless LAN, this product is restricted to indoor use due to its operation in the 5.15- to 5.25-GHz frequency range. Industry Canada requires this product to be used indoors for the frequency range of 5.15 GHz to 5.25 GHz to reduce the potential for harmful interference to co-channel mobile satellite systems. High power radar is allocated as the primary user of the 5.25- to 5.35-GHz and 5.65 to 5.85-GHz bands. These radar stations can cause interference with and/or damage to this device.

The maximum allowed antenna gain for use with this device is 6dBi in order to comply with the E.I.R.P limit for the 5.25- to 5.35 and 5.725 to 5.85 GHz frequency range in point-to-point operation.

This Class B digital apparatus complies with Canadian ICES-003, Issue 4, and RSS-210, No 4 (Dec 2000) and No 5 (Nov 2001).

Cet appareil numérique de la classe B est conforme à la norme NMB-003, No. 4, et CNR-210, No 4 (Dec 2000) et No 5 (Nov 2001).

"To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing."

« Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé a l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence. »

European Union

The low band 5.15 -5.35 GHz is for indoor use only.

Intel(R) WiFi Link 5300 Adapter Declaration of Conformity

The European Declaration of Conformity is available at the following site:

http://www.intel.com/support/go/wireless/wlan/wf_reg.htm

This equipment complies with the essential requirements of the European Union directive 1999/5/EC.

•esky [Czech]	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) WiFi Link 5300 je ve shod• se základními požadavky a dalšími p•íslušnými ustanoveními sm•rnice 1999/5/ES.
Dansk [Danish]	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) WiFi Link 5300 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt Intel(R) Corporation, dass sich das Gerät Intel(R) WiFi Link 5300 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Esti [Estonian]	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) WiFi Link 5300 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, Intel(R) Corporation, declares that this Intel(R) WiFi Link 5300 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente Intel(R) Corporation declara que el Intel(R) WiFi Link 5300 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνικ• [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) WiFi Link 5300 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) WiFi Link 5300 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente Intel(R) Corporation dichiara che questo Intel(R) WiFi Link 5300 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo Intel(R) Corporation deklar•, ka Intel(R) WiFi Link 5300 atbilst Direkt•vas 1999/5/EK b•tiskaj•m pras•b•m un citiem ar to saist•tajiem noteikumiem.
Lietuvi• [Lithuanian]	Šiuo Intel(R) Corporation deklaruoja, kad šis Intel(R) WiFi Link 5300 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) WiFi Link 5300 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Malti [Maltese]	Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) WiFi Link 5300 jikkonforma mal-•ti•ijiet essenzjali u ma provvedimenti o•rajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) WiFi Link 5300 megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Norsk [Norwegian]	Intel Corporation erklærer herved at utstyret Intel(R) WiFi Link 5300 er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.
Polski [Polish]	Niniejszym, Intel(R) Corporation, o•wiadcza, •e Intel(R) WiFi Link 5300 jest zgodne z zasadniczymi wymaganiami oraz innymi stosownymi postanowieniami Dyrektywy 1999/5/WE.
Português [Portuguese]	Intel(R) Corporation declara que este Intel(R) WiFi Link 5300 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	Šiuo Intel(R) Corporation izjavlja, da je ta Intel(R) WiFi Link 5300 v skladu z bistvenimi zahtevami in ostalimi relevantnimi dolo•ili direktive 1999/5/ES.
Slovensky [Slovak]	Intel(R) Corporation týmto vyhlasuje, že Intel(R) WiFi Link 5300 sp••a základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	Intel(R) Corporation vakuuttaa täten että Intel (R) WiFi Link 5300 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar Intel(R) Corporation att denna Intel(R) WiFi Link 5300 står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir Intel(R) Corporation yfir því að Intel(R) WiFi Link 5300 er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.

Intel(R) WiFi Link 5100 Adapter Declaration of Conformity

The European Declaration of Conformity is available at the following site:

http://www.intel.com/support/go/wireless/wlan/wf_reg.htm

This equipment complies with the essential requirements of the European Union directive 1999/5/EC.

•esky [Czech]	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) WiFi Link 5100 je ve shod• se základními požadavky a dalšími p•íslušnými ustanoveními sm•rnice 1999/5/ES.
Dansk [Danish]	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) WiFi Link 5100 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt Intel(R) Corporation, dass sich das Gerät Intel(R) WiFi Link 5100 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Esti [Estonian]	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) WiFi Link 5100 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, Intel(R) Corporation, declares that this Intel(R) WiFi Link 5100 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente Intel(R) Corporation declara que el Intel(R) WiFi Link 5100 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνικ• [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) WiFi Link 5100 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) WiFi Link 5100 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente Intel(R) Corporation dichiara che questo Intel(R) WiFi Link 5100 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo Intel(R) Corporation deklar•, ka Intel(R) WiFi Link 5100 atbilst Direkt•vas 1999/5/EK b•tiskaj•m pras•b•m un citiem ar to saist•tajiem noteikumiem.
Lietuvi• [Lithuanian]	Šiuo Intel(R) Corporation deklaruoja, kad šis Intel(R) WiFi Link 5100 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) WiFi Link 5100 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) WiFi Link 5100 jikkonforma mal-•ti•ijiet essenzjali u ma provvedimenti o•rajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) WiFi Link 5100 megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Norsk [Norwegian]	*Intel Corporation* erklærer herved at utstyret Intel(R) WiFi Link 5100 er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.
Polski [Polish]	Niniejszym, Intel(R) Corporation, o•wiadcza, •e Intel(R) WiFi Link 5100 jest zgodne z zasadniczymi wymaganiami oraz innymi stosownymi postanowieniami Dyrektywy 1999/5/WE.
Português [Portuguese]	Intel(R) Corporation declara que este Intel(R) WiFi Link 5100 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	Šiuo Intel(R) Corporation izjavlja, da je ta Intel(R) WiFi Link 5100 v skladu z bistvenimi zahtevami in ostalimi relevantnimi dolo•ili direktive 1999/5/ES.
Slovensky [Slovak]	Intel(R) Corporation týmto vyhlasuje, že Intel(R) WiFi Link 5100 sp••a základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	Intel(R) Corporation vakuuttaa täten että Intel(R) WiFi Link 5100 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar Intel(R) Corporation att denna Intel(R) WiFi Link 5100 står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir Intel(R) Corporation yfir því að Intel(R) WiFi Link 5100 er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.

Italy

The use of these equipments is regulated by:

1. D.L.gs 1.8.2003, n. 259, article 104 (activity subject to general authorization) for outdoor use and article 105 (free use) for indoor use, in both cases for private use.
2. D.M. 28.5.03, for supply to public of RLAN access to networks and telecom services.

L'uso degli apparati è regolamentato da:

1. D.L.gs 1.8.2003, n. 259, articoli 104 (attività soggette ad autorizzazione generale) se utilizzati al di fuori del proprio fondo e 105 (libero uso) se utilizzati entro il proprio fondo, in entrambi i casi per uso private.
2. D.M. 28.5.03, per la fornitura al pubblico dell'accesso R-LAN alle reti e ai servizi di telecomunicazioni.

Japan

Indoor use only.

Korea

당해 무선설비는 운용 중 전파혼신 가능성이 있음

Morocco

The operation of this product in the radio channel 2 (2417 MHz) is not authorized in the following cities: Agadir, Assa-Zag, Cabo Negro, Chaouen, Goulmima, Oujda, Tan Tan, Taourirt, Taroudant and Taza.

The operation of this product in the radio channels 4, 5, 6 et 7 (2425 - 2442 MHz) is not authorized in the following cities: Aéroport Mohamed V, Agadir, Aguelmous, Anza, Benslimane, Béni Hafida, Cabo Negro, Casablanca, Fès, Lakbab, Marrakech, Merchich, Mohammédia, Rabat, Salé, Tanger, Tan Tan, Taounate, Tit Mellil, Zag.

Taiwan

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Radio Approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed in the manufacturer's OEM Regulatory Guidance document.

Regulatory Markings

A list of required regulatory markings can be found on the web at:

http://support.intel.com/support/wireless/wlan/5100/index.htm

and

http://support.intel.com/support/wireless/wlan/5300/index.htm

---

Intel(R) Wireless WiFi Link 4965AGN and Intel(R) Wireless WiFi Link 4965AG_

The information in this document applies to the following products:

Quad-mode wireless LAN adapters (802.11a/802.11b/802.11g/802.11n)
Intel(R) Wireless WiFi Link 4965AGN (model WM4965AGN)

Tri-mode wireless LAN adapters (802.11a/802.11b/802.11g)
Intel(R) Wireless WiFi Link 4965AG_ (model WM4965AG_)

> **NOTE**: Due to the evolving state of regulations and standards in the wireless LAN field (IEEE 802.11 and similar standards), the information provided herein is subject to change. Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

Information for the User

Safety Notices

USA—FCC and FAA

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The Intel(R) Wireless WiFi Link 4965AGN and Intel(R) Wireless WiFi Link 4965AG_ adapters meet the Human Exposure limits found in OET Bulletin 65, supplement C, 2001, and ANSI/IEEE C95.1, 1992. Proper operation of this radio according to the instructions found in this manual will result in exposure

substantially below the FCC's recommended limits.

The following safety precautions should be observed:

- Do not touch or move antenna while the unit is transmitting or receiving.
- Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; this behavior may cause damage to the radio.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited by the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

Antenna Use

- In order to comply with FCC RF exposure limits, low gain integrated antennas should be located at a minimum distance of 20 cm (8 inches) or more from the body of all persons.
- High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 30 cm (12 inches) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.

Explosive Device Proximity Warning

Warning: Do not operate a portable transmitter (such as a wireless network device) near unshielded blasting caps or in an explosive environment unless the device has been modified to be qualified for such use.

Antenna Warnings

Warning: To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended for the Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ adapters installed in a desktop or portable computer, that the antenna for this device be installed so as to provide a separation distance of al least 20 cm (8 inches) from all persons. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

Warning: Intel(R) PRO/Wireless LAN products are not designed for use with high-gain directional antennas. Use of such antennas with these products in a manner other than as described in the previous section titled, "Antenna Use" is illegal.

Use On Aircraft Caution

Caution: Regulations of the FCC and FAA prohibit airborne operation of radio-frequency wireless devices because their signals could interfere with critical aircraft instruments.

Other Wireless Devices

Safety Notices for Other Devices in the Wireless Network: See the documentation supplied with wireless adapters or other devices in the wireless network.

Local Restrictions on 802.11a, 802.11b, 802.11g and 802.11n Radio Usage

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, 802.11g and 802.11n wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, 802.11g and 802.11n products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. The device transmit power control (TPC) interface is part of the Intel(R) PROSet/Wireless WiFi Connection Utility. Operational restrictions for Equivalent Isotropic Radiated Power (EIRP) are provided by the system manufacturer. Any deviation from the permissible power and frequency settings for the country of use is an infringement of national law and may be

punished as such.

For country-specific information, see the additional compliance information supplied with the product.

Wireless Interoperability

The Intel(R) Wireless WiFi Link 4965AGN and Intel(R) Wireless WiFi Link 4965AG_ adapters are designed to be interoperable with other wireless LAN products that are based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

- IEEE Std. 802.11b compliant Standard on Wireless LAN
- IEEE Std. 802.11g compliant Standard on Wireless LAN
- IEEE Std. 802.11a compliant Standard on Wireless LAN
- IEEE Std. 802.11n draft 2.0 compliant on Wireless LAN (does apply to the Intel(R) Wireless WiFi Link 4965AG_ adapter)
- Wireless Fidelity certification, as defined by the Wi-Fi Alliance

The Intel(R) Wireless WiFi Link 4965AGN Adapter or Intel(R) Wireless WiFi Link 4965AG_ Adapter and Your Health

The Intel(R) Wireless WiFi Link 4965AGN adapter and Intel(R) Wireless WiFi Link 4965AG_ adapter, like other radio devices, emit radio frequency electromagnetic energy. The level of energy emitted by the device, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The adapter operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the Intel (R) Wireless WiFi Link 4965AGN adapter or Intel(R) Wireless WiFi Link 4965AG_ adapter may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:

- Using the adapter equipment on board airplanes, or
- Using the adapter equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the Intel(R) Wireless WiFi Link 4965AGN or Intel (R) Wireless WiFi Link 4965AG_ adapter before you turn it on.

Regulatory Information

Information for the OEMs and Integrators

The following statement must be included with all versions of this document supplied to an OEM or integrator, but should not be distributed to the end user.

- This device is intended for OEM integrators only.
- Please see the full Grant of Equipment document for other restrictions.
- This device must be operated and used with a locally approved access point.

Information To Be Supplied to the End User by the OEM or Integrator

The following regulatory and safety notices must be published in documentation supplied to the end user of the product or system incorporating an Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ in compliance with local regulations. Host system must be labeled with "Contains FCC ID: XXXXXXXX", FCC ID displayed on label.

The Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific approvals, see Radio Approvals. Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized

modification, substitution or attachment is the responsibility of the user. Intel Corporation and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

Local Restriction of 802.11a, 802.11b, 802.11g, and 802.11n Radio Usage

The following statement on local restrictions must be published as part of the compliance documentation for all 802.11a, 802.11b, 802.11g and 802.11n products.

⚠ **Caution**: Due to the fact that the frequencies used by 802.11a, 802.11b, 802.11g and 802.11n wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, 802.11g and 802.11n products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. Any deviation from permissible settings and restrictions in the country of use could be an infringement of national law and may be punished as such.

FCC Radio Frequency Interference Requirements

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. FCC requires this product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems. High power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with and /or damage this device.

- This device is intended for OEM integrators only.

USA—Federal Communications Commission (FCC)

This device complies with Part 15 of the FCC Rules. Operation of the device is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

> **NOTE**: The radiated output power of the Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ adapter is far below the FCC radio frequency exposure limits. Nevertheless, the Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ adapter should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 20 cm between you (or any other person in the vicinity) and the antenna that is built into the computer. Details of the authorized configurations can be found at http://www.fcc.gov/oet/ea/ by entering the FCC ID number on the device.

Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If the equipment is not installed and used in accordance with the instructions, the equipment may cause harmful interference to radio communications. There is no guarantee, however, that such interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

> **NOTE**: The Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ adapter must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations.

Underwriters Laboratories Inc. (UL) Regulatory Warning

For use in (or with) UL Listed personal computers or compatible.

Brazil

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Canada—Industry Canada (IC)

This device complies with RSS210 of Industry Canada.

⚠ **Caution**: When using IEEE 802.11a wireless LAN, this product is restricted to indoor use due to its operation in the 5.15- to 5.25-GHz frequency range. Industry Canada requires this product to be used indoors for the frequency range of 5.15 GHz to 5.25 GHz to reduce the potential for harmful interference to co-channel mobile satellite systems. High power radar is allocated as the primary user of the 5.25- to 5.35-GHz and 5.65 to 5.85-GHz bands. These radar stations can cause interference with and/or damage to this device.

The maximum allowed antenna gain for use with this device is 6dBi in order to comply with the E.I.R.P limit for the 5.25- to 5.35 and 5.725 to 5.85 GHz frequency range in point-to-point operation.

This Class B digital apparatus complies with Canadian ICES-003, Issue 4, and RSS-210, No 4 (Dec 2000) and No 5 (Nov 2001).

Cet appareil numérique de la classe B est conforme à la norme NMB-003, No. 4, et CNR-210, No 4 (Dec 2000) et No 5 (Nov 2001).

"To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing."

« Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé a l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence. »

European Union

The low band 5.15 -5.35 GHz is for indoor use only.

Declaration of Conformity

The European Declaration of Conformity is available at the following site:

http://download.intel.com/support/wireless/wlan/4965agn/sb/eudoc4965_combined1.pdf

This equipment complies with the essential requirements of the European Union directive 1999/5/EC.

•esky [Czech]	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ je ve shod• se základními požadavky a dalšími p•íslušnými ustanoveními sm•rnice 1999/5/ES.
Dansk [Danish]	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt Intel(R) Corporation, dass sich das Gerät Intel(R) Wireless WiFi Link 4965AGN or Intel (R) Wireless WiFi Link 4965AG_ in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

Esti [Estonian]	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, Intel(R) Corporation, declares that this Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente Intel(R) Corporation declara que el Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνικ• [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente Intel(R) Corporation dichiara che questo Intel(R) Wireless WiFi Link 4965AGN or Intel (R) Wireless WiFi Link 4965AG_ è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo Intel(R) Corporationdeklar•, ka Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ atbilst Direkt•vas 1999/5/EK b•tiskaj•m pras•b•m un citiem ar to saist•tajiem noteikumiem.
Lietuvi• [Lithuanian]	Šiuo Intel(R) Corporation deklaruoja, kad šis Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ jikkonforma mal-•ti•ijiet essenzjali u ma provvedimenti o•rajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Norsk [Norwegian]	*Intel Corporation* erklærer herved at utstyretIntel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.
Polski [Polish]	Niniejszym, Intel(R) Corporation, o•wiadcza, •e Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ jest zgodne z zasadniczymi wymaganiami oraz innymi stosownymi postanowieniami Dyrektywy 1999/5/WE.
Português [Portuguese]	Intel(R) Corporation declara que este Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	Šiuo Intel(R) Corporation izjavlja, da je ta Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ v skladu z bistvenimi zahtevami in ostalimi relevantnimi dolo•ili direktive 1999/5/ES.
Slovensky [Slovak]	Intel(R) Corporation týmto vyhlasuje, že Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ sp••a základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	Intel(R) Corporation vakuuttaa täten että Intel (R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar Intel(R) Corporation att denna Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir Intel(R) Corporation yfir því að Intel(R) Wireless WiFi Link 4965AGN or Intel(R) Wireless WiFi Link 4965AG_ er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.

Italy

The use of these equipments is regulated by:

1. D.L.gs 1.8.2003, n. 259, article 104 (activity subject to general authorization) for outdoor use and article 105 (free use) for indoor use, in both cases for private use.
2. D.M. 28.5.03, for supply to public of RLAN access to networks and telecom services.

L'uso degli apparati è regolamentato da:

1. D.L.gs 1.8.2003, n. 259, articoli 104 (attività soggette ad autorizzazione generale) se utilizzati al di fuori del proprio fondo e 105 (libero uso) se utilizzati entro il proprio fondo, in entrambi i casi per uso private.
2. D.M. 28.5.03, per la fornitura al pubblico dell'accesso R-LAN alle reti e ai servizi di telecomunicazioni.

Japan

Indoor use only.

Korea

당해 무선설비는 운용 중 전파혼신 가능성이 있음

Taiwan

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Radio Approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed in the manufacturer's OEM Regulatory Guidance document.

Regulatory Markings

A list of required regulatory markings can be found on the web at:

> http://www.intel.com/network/connectivity/resources/doc_library/regulatory/regulatory_markings_4965AGN.htm.

Intel(R) PRO/Wireless 3945ABG Network Connection and the Intel(R) PRO/Wireless 3945BG Network Connection

The information in this document applies to the following products:

Tri-mode wireless LAN adapters (802.11a/802.11b/802.11g)
Intel(R) PRO/Wireless 3945ABG Network Connection (model WM3945ABG)

Dual-mode wireless LAN adapters (802.11b/802.11g)
Intel(R) PRO/Wireless 3945BG Network Connection (model WM3945BG)

> **NOTE**: Due to the evolving state of regulations and standards in the wireless LAN field (IEEE 802.11 and similar standards), the information provided herein is subject to change. Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

Information for the User

Safety Notices

USA—FCC and FAA

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The Intel(R) PRO/Wireless 3945ABG Network Connection adapter, or the Intel(R) PRO/Wireless 3945BG Network Connection adapter meet the Human Exposure limits found in OET Bulletin 65, supplement C, 2001, and ANSI/IEEE C95.1, 1992. Proper operation of this radio according to the instructions found in this manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

- Do not touch or move antenna while the unit is transmitting or receiving.
- Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; this behavior may cause damage to the radio.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited by the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

Antenna Use

- In order to comply with FCC RF exposure limits, low gain integrated antennas should be located at a minimum distance of 20 cm (8 inches) or more from the body of all persons.
- High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 30 cm (12 inches) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.

Explosive Device Proximity Warning

Warning: Do not operate a portable transmitter (such as a wireless network device) near unshielded blasting caps or in an explosive environment unless the device has been modified to be qualified for such use.

Antenna Warnings

Warning: To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended that when the Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection adapter is installed in a desktop or portable computer, the antenna for this device be installed so as to provide a separation distance of al least 20 cm (8 inches) from all persons. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

Warning: Intel(R) PRO/Wireless LAN products are not designed for use with high-gain directional antennas. Use of such antennas with these products in a manner other than as described in the previous section titled, "Antenna Use" is

illegal.

Use On Aircraft Caution

⚠ **Caution**: Regulations of the FCC and FAA prohibit airborne operation of radio-frequency wireless devices because their signals could interfere with critical aircraft instruments.

Other Wireless Devices

Safety Notices for Other Devices in the Wireless Network: See the documentation supplied with wireless adapters or other devices in the wireless network.

Local Restrictions on 802.11a, 802.11b, and 802.11g Radio Usage

⚠ **Caution**: Due to the fact that the frequencies used by 802.11a, 802.11b and 802.11g wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, and 802.11g products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. The device transmit power control (TPC) interface is part of the Intel(R) PROSet/Wireless WiFi Connection Utility. Operational restrictions for Equivalent Isotropic Radiated Power (EIRP) are provided by the system manufacturer. Any deviation from the permissible power and frequency settings for the country of use is an infringement of national law and may be punished as such.

For country-specific information, see the additional compliance information supplied with the product.

Wireless Interoperability

The Intel(R) PRO/Wireless 3945ABG Network Connection and Intel(R) PRO/Wireless 3945BG Network Connection are designed to be interoperable with other wireless LAN products that are based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

- IEEE Std. 802.11b compliant Standard on Wireless LAN
- IEEE Std. 802.11g compliant Standard on Wireless LAN
- IEEE Std. 802.11a compliant Standard on Wireless LAN
- Wireless Fidelity (Wi-Fi) certification, as defined by the Wi-Fi Alliance

The Intel(R) PRO/Wireless 3945ABG Network Connection Adapter or the Intel(R) PRO/Wireless 3945BG Network Connection Adapter and Your Health

The Intel(R) PRO/Wireless 3945ABG Network Connection adapter or the Intel(R) PRO/Wireless 3945BG Network Connection adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by this device, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The Intel(R) PRO/Wireless 3945ABG Network Connection adapter or the Intel(R) PRO/Wireless 3945BG Network Connection adapter wireless device operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the Intel(R) PRO/Wireless 3945ABG Network Connection adapter or the Intel(R) PRO/Wireless 3945BG Network Connection adapter may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:

- Using the Intel(R) PRO/Wireless 3945ABG Network Connection adapter or the Intel(R) PRO/Wireless 3945BG Network Connection adapter equipment on board airplanes, or
- Using the Intel(R) PRO/Wireless 3945ABG Network Connection adapter or the Intel(R) PRO/Wireless 3945BG Network Connection adapter equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the Intel(R) PRO/Wireless 3945ABG Network Connection adapter or the Intel(R) PRO/Wireless 3945BG Network Connection wireless devices before you turn it on.

Regulatory Information

Information for the OEMs and Integrators

The following statement must be included with all versions of this document supplied to an OEM or integrator, but should not be distributed to the end user.

- This device is intended for OEM integrators only.
- Please see the full Grant of Equipment document for other restrictions.
- This device must be operated and used with a locally approved access point.

Information To Be Supplied to the End User by the OEM or Integrator

The following regulatory and safety notices must be published in documentation supplied to the end user of the product or system incorporating an Intel(R) PRO/Wireless 3945ABG Network Connection or an Intel(R) PRO/Wireless 3945BG Network Connection in compliance with local regulations. Host system must be labeled with "Contains FCC ID: XXXXXXXX", FCC ID displayed on label.

The Intel(R) PRO/Wireless 3945ABG Network Connection adapter or the Intel(R) PRO/Wireless 3945BG Network Connection wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific approvals, see Radio Approvals. Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel(R) PRO/Wireless 3945ABG Network Connection or the Intel(R) PRO/Wireless 3945BG Network Connection adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

Local Restriction of 802.11a, 802.11b, and 802.11g Radio Usage

The following statement on local restrictions must be published as part of the compliance documentation for all 802.11a, 802.11b, and 802.11g products.

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, and 802.11g wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, and 802.11g products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. Any deviation from permissible settings and restrictions in the country of use could be an infringement of national law and may be punished as such.

FCC Radio Frequency Interference Requirements

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. FCC requires this product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems. High power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with and /or damage this device.

- This device is intended for OEM integrators only.

USA—Federal Communications Commission (FCC)

This device complies with Part 15 of the FCC Rules. Operation of the device is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

NOTE: The radiated output power of the Intel(R) PRO/Wireless 3945ABG Network Connection adapter or the Intel(R) PRO/Wireless 3945BG Network Connection adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel(R) PRO/Wireless LAN wireless network device should be

used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 20 cm between you (or any other person in the vicinity) and the antenna that is built into the computer. Details of the authorized configurations can be found at http://www.fcc.gov/oet/ea/ by entering the FCC ID number on the device.

Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If the equipment is not installed and used in accordance with the instructions, the equipment may cause harmful interference to radio communications. There is no guarantee, however, that such interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

NOTE: The Intel(R) PRO/Wireless 3945ABG Network Connection adapter or the Intel(R) PRO/Wireless 3945BG Network Connection adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations.

Underwriters Laboratories Inc. (UL) Regulatory Warning

For use in (or with) UL Listed personal computers or compatible.

Brazil

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Canada—Industry Canada (IC)

This device complies with RSS210 of Industry Canada.

Caution: When using IEEE 802.11a wireless LAN, this product is restricted to indoor use due to its operation in the 5.15- to 5.25-GHz frequency range. Industry Canada requires this product to be used indoors for the frequency range of 5.15 GHz to 5.25 GHz to reduce the potential for harmful interference to co-channel mobile satellite systems. High power radar is allocated as the primary user of the 5.25- to 5.35-GHz and 5.65 to 5.85-GHz bands. These radar stations can cause interference with and/or damage to this device.

The maximum allowed antenna gain for use with this device is 6dBi in order to comply with the E.I.R.P limit for the 5.25- to 5.35 and 5.725 to 5.85GHz frequency range in point-to-point operation.

This Class B digital apparatus complies with Canadian ICES-003, Issue 4, and RSS-210, No 4 (Dec 2000) and No 5 (Nov 2001).

Cet appareil numérique de la classe B est conforme à la norme NMB-003, No. 4, et CNR-210, No 4 (Dec 2000) et No 5 (Nov 2001).

"To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing."

« Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé a l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne

d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence.»

European Union

The low band 5.15 -5.35 GHz is for indoor use only.

Declaration of Conformity

Declaration of Conformity (1999/5/EC)

We, **INTEL CORPORATION SAS**
Address: Les Taissounières B3, 1681 route des Dolines – BP 293
06905 – Sophia Antipolis, France

declare under our sole responsibility that the product:

- Name: **INTEL® PRO/Wireless 3945ABG Network Connection**
- Model: **WM3945ABG** MOW2

to which this declaration relates, is in compliance with all the applicable essential requirements, and other provisions of the European Council Directive:

1999/5/EC	Radio and Telecommunications Terminal Equipment Directive (R&TTE)

The conformity assessment procedure used for this declaration is Annex IV of this Directive

This product will bear the CE Mark label CE 0336 !

Product compliance has been demonstrated on the basis of:

- IEC 60950-1:2001, and EN 60950-1: 2001 (safety) - EN 50371: 2002	For article 3.1(a) : Health and Safety of the User
- EN 301 489-1 V1.4.1 (2002-08) - EN 301 489-17 V1.2.1 (2002-08)	For article 3.1(b) : Electromagnetic Compatibility
- EN 300 328 V1.5.1 (2004-08) - EN 301 893 V1.2.3 (2003-08)	For article 3.2 : Effective use of the spectrum allocated

The technical construction file is kept available at:

- EN 301 893 V1.2.3 (2003-08)	For article 3.2 : Effective use of the spectrum allocated

The technical construction file is kept available at:

INTEL CORPORATION SAS
Branch Office: 1681 route des Dolines,
06905 - Sophia Antipolis, France

Authorized Signature by   Date: 9th September 2005



Gilles Catala,
Regulatory & Compliance Engineering Manager
Wireless Networking Group

This equipment complies with the essential requirements of the European Union directive 1999/5/EC.

•esky [Czech]	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection je ve shod• se základními požadavky a dalšími p•íslušnými ustanoveními sm•rnice 1999/5/ES.
Dansk [Danish]	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt Intel(R) Corporation, dass sich das Gerät Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Esti [Estonian]	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, Intel(R) Corporation, declares that this Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente Intel(R) Corporation declara que el Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνικ• [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente Intel(R) Corporation dichiara che questo Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo Intel(R) Corporationdeklar•, ka Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection atbilst Direkt•vas 1999/5/EK b•tiskaj•m pras•b•m un citiem ar to saist•tajiem noteikumiem.
Lietuvi• [Lithuanian]	Šiuo Intel(R) Corporation deklaruoja, kad šis Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection jikkonforma mal-•ti•ijiet essenzjali u ma provvedimenti o•rajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Norsk [Norwegian]	*Intel Corporation* erklærer herved at utstyret Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.
Polski [Polish]	Niniejszym, Intel(R) Corporation, o•wiadcza, •e Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection jest zgodne z zasadniczymi wymaganiami oraz innymi stosownymi postanowieniami Dyrektywy 1999/5/WE.
Português [Portuguese]	Intel(R) Corporation declara que este Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	Šiuo Intel(R) Corporation izjavlja, da je ta Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection v skladu z bistvenimi zahtevami in ostalimi relevantnimi dolo•ili direktive 1999/5/ES.
Slovensky [Slovak]	Intel(R) Corporation týmto vyhlasuje, že Intel(R) PRO/Wireless 3945ABG Network Connection or Intel (R) PRO/Wireless 3945BG Network Connection sp••a základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	Intel(R) Corporation vakuuttaa täten että Intel(R) PRO/Wireless 3945ABG Network Connection or Intel (R) PRO/Wireless 3945BG Network Connection tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar Intel(R) Corporation att denna Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir Intel(R) Corporation yfir því að Intel(R) PRO/Wireless 3945ABG Network Connection or Intel(R) PRO/Wireless 3945BG Network Connection) er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.

Italy

The use of these equipments is regulated by:

1. D.L.gs 1.8.2003, n. 259, article 104 (activity subject to general authorization) for outdoor use and article 105 (free use) for indoor use, in both cases for private use.
2. D.M. 28.5.03, for supply to public of RLAN access to networks and telecom services.

L'uso degli apparati è regolamentato da:

1. D.L.gs 1.8.2003, n. 259, articoli 104 (attività soggette ad autorizzazione generale) se utilizzati al di fuori del proprio fondo e 105 (libero uso) se utilizzati entro il proprio fondo, in entrambi i casi per uso privato.
2. D.M. 28.5.03, per la fornitura al pubblico dell'accesso R-LAN alle reti e ai servizi di telecomunicazioni.

Japan

Indoor use only.

Korea

당해 무선설비는 운용 중 전파혼신 가능성이 있음

Taiwan

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Radio Approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed in the manufacturer's OEM Regulatory Guidance document.

Intel(R) PRO/Wireless 2915ABG Network Connection

The information in this document applies to the following products:

Tri-mode wireless LAN adapters (802.11a/802.11b/802.11g)
Intel(R) PRO/Wireless 2915ABG Network Connection (model WM3B2915ABG)
Intel(R) PRO/Wireless 2915ABG Network Connection (model WM3A2915ABG)

> **NOTE**: Due to the evolving state of regulations and standards in the wireless LAN field (IEEE 802.11 and similar standards), the information provided herein is subject to change. Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

Information for the User

Safety Notices

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The Intel(R) PRO/Wireless 2915ABG Network Connection adapter meets the Human Exposure limits found in OET Bulletin 65, supplement C, 2001, and ANSI/IEEE C95.1, 1992. Proper operation of this radio according to the instructions found in this manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

- Do not touch or move antenna while the unit is transmitting or receiving.
- Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; this behavior may cause damage to the radio.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited by the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

Antenna Use

- In order to comply with FCC RF exposure limits, low gain integrated antennas should be located at a minimum distance of 20 cm (8 inches) or more from the body of all persons.
- High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 30 cm (12 inches) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.

Explosive Device Proximity Warning

Warning: Do not operate a portable transmitter (such as a wireless network device) near unshielded blasting caps or in an explosive environment unless the device has been modified to be qualified for such use.

Antenna Warnings

Warning: To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended that when the Intel(R) PRO/Wireless 2915ABG Network Connection adapter is installed in a desktop or portable computer, the antenna for this device be installed so as to provide a separation distance of al least 20 cm (8 inches) from all persons. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

Warning: Intel(R) PRO/Wireless LAN products are not designed for use with high-gain directional antennas. Use of such antennas with these products in a manner other than as described in the previous section titled, “Antenna Use” is illegal.

Use On Aircraft Caution

Caution: Regulations of the FCC and FAA prohibit airborne operation of radio-frequency wireless devices because their signals could interfere with critical aircraft instruments.

Other Wireless Devices

Safety Notices for Other Devices in the Wireless Network: See the documentation supplied with wireless adapters or other devices in the wireless network.

Local Restrictions on 802.11a, 802.11b, and 802.11g Radio Usage

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, and 802.11g wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, and 802.11g products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. The device transmit power control (TPC) interface is part of the Intel(R) PROSet/Wireless WiFi Connection Utility. Operational restrictions for Equivalent Isotropic Radiated Power (EIRP) are provided by the system manufacturer. Any deviation from the permissible power and frequency settings for the country of use is an infringement of national law and may be punished as such.

For country-specific information, see the additional compliance information supplied with the product.

Wireless Interoperability

The Intel(R) PRO/Wireless 2915ABG Network Connection adapter is designed to be interoperable with other wireless LAN products that are based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

- IEEE Std. 802.11b compliant Standard on Wireless LAN.
- IEEE Std. 802.11g compliant Standard on Wireless LAN.
- IEEE Std. 802.11a compliant Standard on Wireless LAN.
- Wireless Fidelity (Wi-Fi) certification, as defined by the Wi-Fi Alliance

The Intel(R) PRO/ Wireless 2915ABG Network Connection Adapter and Your Health

The Intel(R) PRO/Wireless 2915ABG Network Connection adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by this device, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The Intel(R) PRO/Wireless 2915ABG Network Connection adapter wireless device operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the Intel(R) PRO/Wireless 2915ABG Network Connection adapter wireless device may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:

- Using the Intel(R) PRO/Wireless 2915ABG Network Connection adapter equipment on board airplanes, or
- Using the Intel(R) PRO/Wireless 2915ABG Network Connection adapter equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the Intel(R) PRO/Wireless 2915ABG Network Connection adapter wireless device before you turn it on.

Regulatory Information

Information for the OEMs and Integrators

The following statement must be included with all versions of this document supplied to an OEM or integrator, but should not be distributed to the end user.

- This device is intended for OEM integrators only.
- Please see the full Grant of Equipment document for other restrictions.
- This device must be operated and used with a locally approved access point.

Information To Be Supplied to the End User by the OEM or Integrator

The following regulatory and safety notices must be published in documentation supplied to the end user of the product or system incorporating an Intel(R) PRO/Wireless 2915ABG Network Connection in compliance with local regulations. Host system must be labeled with "Contains FCC ID: XXXXXXXX", FCC ID displayed on label.

The Intel(R) PRO/Wireless 2915ABG Network Connection adapter must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific approvals, see Radio Approvals. Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel(R) PRO/Wireless 2915ABG Network Connection adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

Local Restriction of 802.11a, 802.11b, and 802.11g Radio Usage

The following statement on local restrictions must be published as part of the compliance documentation for all 802.11a, 802.11b, and 802.11g products.

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, and 802.11g wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, and 802.11g products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. Any deviation from permissible settings and restrictions in the country of use could be an infringement of national law and may be punished as such.

FCC Radio Frequency Interference Requirements

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. FCC requires this

product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems. High power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with and /or damage this device.

- This device is intended for OEM integrators only.

USA—Federal Communications Commission (FCC)

This device complies with Part 15 of the FCC Rules. Operation of the device is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

> **NOTE**: The radiated output power of the Intel(R) PRO/Wireless 2915ABG Network Connection adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel(R) PRO/Wireless LAN wireless network device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 20 cm between you (or any other person in the vicinity) and the antenna that is built into the computer.

Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If the equipment is not installed and used in accordance with the instructions, the equipment may cause harmful interference to radio communications. There is no guarantee, however, that such interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

> **NOTE**: The Intel(R) PRO/Wireless 2915ABG Network Connection adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations.

Canada—Industry Canada (IC)

This device complies with RSS210 of Industry Canada.

This Class B digital apparatus complies with Canadian ICES-003, Issue 4, and RSS-210, No 4 (Dec 2000) and No 5 (Nov 2001).

Cet appareil numérique de la classe B est conforme à la norme NMB-003, No. 4, et CNR-210, No 4 (Dec 2000) et No 5 (Nov 2001).

"To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing."

« Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé a l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence. »

European Union

The low band 5.15 -5.35 GHz is for indoor use only.

Declaration of Conformity (1999/5/EC)

We, **INTEL CORPORATION SA**
Address: Branch Office; Veldkant 31; 2550 Kontich, Belgium

declare under our sole responsibility that the product:
- Name: **INTEL® PRO/Wireless 2915ABG Network Connection**
- Model: **WM3B2915ABG EU**

to which this declaration relates, is in compliance with all the applicable essential requirements, and other provisions of the European Council Directive:

1999/5/EC	Radio and Telecommunications Terminal Equipment Directive (R&TTE)

The conformity assessment procedure used for this declaration is Annex IV of this Directive

This product will bear the CE Mark label CE 0523 !

Product compliance has been demonstrated on the basis of:

- IEC 60950 (1999 3rd Edition with amendments 1, 2, 3, 4), and EN 60950 (2000) - 1995/519/EC, Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)	For article 3.1(a) : Health and Safety of the User
- EN 301 489-1 v1.4.1, Aug. 2002 - EN 301 489-17 v1.2.1, Aug. 2002	For article 3.1(b) : Electromagnetic Compatibility
- Final Draft EN 300 328 v1.5.1, Mar 2004 - EN 301 893 v1.2.3, Aug 2003	For article 3.2 : Effective use of the spectrum allocated

The technical construction file is kept available at:

INTEL CORPORATION SA
Branch Office: Veldkant 31,

The technical construction file is kept available at:

INTEL CORPORATION SA
Branch Office: Veldkant 31,
2550 Kontich, Belgium

Authorized Signature by

Date: July 19th 2004



Vincent Colin,
Worldwide Homologations Manager,
WPD Regulatory Department

Declaration of Conformity (1999/5/EC)

We, **INTEL CORPORATION SA**
Address: Branch Office; Veldkant 31; 2550 Kontich, Belgium

declare under our sole responsibility that the product:

- Name: **INTEL® PRO/Wireless 2915ABG Network Connection**
- Model: **WM3A2915ABG EU**

to which this declaration relates, is in compliance with all the applicable essential requirements, and other provisions of the European Council Directive:

1999/5/EC	Radio and Telecommunications Terminal Equipment Directive (R&TTE)

The conformity assessment procedure used for this declaration is Annex IV of this Directive

This product will bear the CE Mark label CE 0523 !

Product compliance has been demonstrated on the basis of:

- IEC 60950 (1999 3rd Edition with amendments 1, 2, 3, 4), and EN 60950 (2000) - 1995/519/EC, Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)	For article 3.1(a) : Health and Safety of the User

(2000) - 1995/519/EC, Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)	For article 3.1(a) : Health and Safety of the User
- EN 301 489-1 v1.4.1, Aug. 2002 - EN 301 489-17 v1.2.1, Aug. 2002	For article 3.1(b) : Electromagnetic Compatibility
- Final Draft EN 300 328 v1.5.1, Mar 2004 - EN 301 893 v1.2.3, Aug 2003	For article 3.2 : Effective use of the spectrum allocated

The technical construction file is kept available at:

INTEL CORPORATION SA
Branch Office: Veldkant 31,
2550 Kontich, Belgium

Authorized Signature by

Date: July 19th 2004

Vincent Colin,
Worldwide Homologations Manager,
WPD Regulatory Department

This equipment complies with the essential requirements of the European Union directive 1999/5/EC.

Czech	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) PRO/Wireless 2915ABG Network Connection je ve shod• se základními požadavky a dalšími p•íslušnými ustanoveními sm•rnice 1999/5/ES."
Danish	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) PRO/Wireless 2915ABG Network Connection overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
Dutch	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) PRO/Wireless 2915ABG Network Connection in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
	Bij deze verklaart Intel(R) Corporation dat deze Intel(R) PRO/Wireless 2915ABG Network Connection voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
English	Hereby, Intel(R) Corporation, declares that this Intel(R) PRO/Wireless 2915ABG Network Connection is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Estonian	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) PRO/Wireless 2915ABG Network Connection vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish	Intel(R) Corporation vakuuttaa täten että Intel(R) PRO/Wireless 2915ABG Network Connection tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

French	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) PRO/Wireless 2915ABG Network Connection est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
	Par la présente, Intel(R) Corporation déclare que ce Intel(R) PRO/Wireless 2915ABG Network Connection est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
German	Hiermit erklärt Intel(R) Corporation, dass sich dieser/diese/dieses Intel(R) PRO/Wireless 2915ABG Network Connection in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)
	Hiermit erklärt Intel(R) Corporation die Übereinstimmung des Gerätes Intel(R) PRO/Wireless 2915ABG Network Connection mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien).=
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) PRO/Wireless 2915ABG Network Connection ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Hungarian	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) PRO/Wireless 2915ABG Network Connection megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Icelandic	*Intel* lysir her med yfir að thessi bunadur, Intel(R) PRO/Wireless 2915ABG Network Connection , uppfyllir allar grunnkrofur, sem gerdar eru i R&TTE tilskipun ESB nr 1999/5/EC
Italian	Con la presente Intel(R) Corporation dichiara che questo Intel(R) PRO/Wireless 2915ABG Network Connection è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian	Ar šo Intel(R) Corporationdeklar•, ka Intel(R) PRO/Wireless 2915ABG Network Connection atbilst Direkt•vas 1999/5/EK b•tiskaj•m pras•b•m un citiem ar to saist•tajiem noteikumiem.
Lithuanian	Intel(R) Corporation deklaruoja, kad Intel(R) Pro/Wireless 2915ABG Network Connectionatitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas".
Malti	Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) PRO/Wireless 2915ABG Network Connection jikkonforma mal-•ti•ijiet essenzjali u ma provvedimenti o•rajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Polish	Niniejszym, Intel(R) Corporation, deklaruj•, •e Intel(R) PRO/Wireless 2915ABG Network Connection spe•nia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.
Portuguese	Intel(R) Corporation declara que este Intel(R) PRO/Wireless 2915ABG Network Connection está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovak	Intel(R) Corporation týmto vyhlasuje, že Intel(R) PRO/Wireless 2915ABG Network Connection sp••a základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenia	Šiuo Intel(R) Corporation deklaruoja, kad šis Intel(R) PRO/Wireless 2915ABG Network Connection atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Spanish	Por medio de la presente Intel(R) Corporation declara que el Intel(R) PRO/Wireless 2915ABG Network Connection cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Swedish	Härmed intygar Intel(R) Corporation att denna Intel(R) PRO/Wireless 2915ABG Network Connection står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

France

Pour la France métropolitaine
2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
2.400 -2.454 GHz (canaux 1 à 7) autorisé en usage extérieur

Pour la Guyane et la Réunion
2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
2.420 - 2.4835 GHz (canaux 5 à 13) autorisé en usage extérieur

Pour tout le territoire Français:

Seulement 5.15 -5.35 GHz autorisé pour le 802.11a

Belgium

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

In geval van privé-gebruik, buiten een gebouw, op een openbare plaats, is geen registratie nodig, wanneer de afstand minder dan 300m is. Voor een afstand groter dan 300m is een registratie bij BIPT vereist. Voor registraties en licenties, gelieve BIPT te contacteren.

Japan

5GHz 帯は室内でのみ使用のこと

Italy

The use of these equipments is regulated by:

- D.L.gs 1.8.2003, n. 259, article 104 (activity subject to general authorization) for outdoor use and article 105 (free use) for indoor use, in both cases for private use.

- D.M. 28.5.03, for supply to public of RLAN access to networks and telecom services.

L’uso degli apparati è regolamentato da:

- D.L.gs 1.8.2003, n. 259, articoli 104 (attività soggette ad autorizzazione generale) se utilizzati al di fuori del proprio fondo e 105 (libero uso) se utilizzati entro il proprio fondo, in entrambi i casi per uso privato.

- D.M. 28.5.03, per la fornitura al pubblico dell’accesso R-LAN alle reti e ai servizi di telecomunicazioni.

Greece

A license is required for the outdoor use of band 5.470 – 5.725 GHz.

Belarus

2.4 GHz OFDM (802.11g) is not allowed at this time.

Indonesia

5 GHz interface is not allowed at this time.

Kuwait

5 GHz interface is not allowed at this time.

Oman

If the modules are less than 100 milliwatts they are unlicensed but if they are more than 100 milliwatts, the user is responsible for getting a license to operate from Telecommunications Regulatory Authority (TRA) in Sultanate of Oman.

Taiwan

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Pakistan

Pakistan Telecommunication Authority (PTA) Approved

UAE

5 GHz interface is not allowed at this time.

Ukraine

5 GHz interface is not allowed at this time.

Radio Approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed in the manufacturer's OEM Regulatory Guidance document.

Underwriters Laboratories Inc. (UL) Regulatory Warning

For use in (or with) UL Listed personal computers or compatible.

Intel(R) PRO/Wireless 2200BG Network Connection

Information for the User

Safety Notices

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The Intel(R) PRO/Wireless 2200BG Network Connection meets the Human Exposure limits found in OET Bulletin 65, 2001, and ANSI/IEEE C95.1, 1992. Proper operation of this radio according to the instructions found in this manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

- Do not touch or move antenna while the unit is transmitting or receiving.
- Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; this behavior may cause damage to the radio.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited by the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

Antenna Use

- In order to comply with FCC RF exposure limits, low gain integrated antennas should be located at a minimum distance of 20 cm (8 inches) or more from the body of all persons.
- High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 30 cm (12 inches) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.

Explosive Device Proximity Warning

Warning: Do not operate a portable transmitter (such as a wireless network device) near unshielded blasting caps or in an explosive environment unless the device has been modified to be qualified for such use.

Antenna Warnings

Warning: To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended that when the Intel(R) PRO/Wireless 2200BG Network Connection adapter is installed in a desktop or portable computer, the antenna for this device be installed so as to provide a separation distance of al least 20 cm (8 inches) from all persons. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

Warning: Intel(R) PRO/Wireless LAN products are not designed for use with high-gain directional antennas. Use of such antennas with these products in a manner other than as described in the previous section titled, "Antenna Use" is illegal.

Use On Aircraft Caution

Caution: Regulations of the FCC and FAA prohibit airborne operation of radio-frequency wireless devices because their signals could interfere with critical aircraft instruments.

Local Restrictions on 802.11b and 802.11g Radio Usage

All frequencies used by 802.11b and 802.11g are harmonized. Some countries though may not allow 802.11g.

Wireless Interoperability

The Intel(R) PRO/Wireless 2200BG Network Connection adapter is designed to be interoperable with any wireless LAN product that is based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

- IEEE Std. 802.11b-1999. Standard on Wireless LAN.
- IEEE Std. 802.11g compliant. Standard on Wireless LAN.
- Wireless Fidelity (Wi-Fi) certification, as defined by the Wi-Fi Alliance

The Intel(R) PRO/Wireless LAN 2200BG Mini PCI Adapter and Your Health

The Intel(R) PRO/Wireless 2200BG Network Connection adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by this device, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless device operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless device may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:

- Using the Intel(R) PRO/Wireless 2200BG Network Connection adapter equipment on board airplanes, or
- Using the Intel(R) PRO/Wireless 2200BG Network Connection adapter equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless device before you turn it on.

Regulatory Information

The Intel(R) PRO/Wireless 2200BG Network Connection adapter must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific approvals, see Radio Approvals. Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel(R) PRO/Wireless 2200BG Network Connection adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

USA—Federal Communications Commission (FCC)

This device complies with Part 15 of the FCC Rules. Operation of the device is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

    NOTE: The radiated output power of the Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel(R) PROSet/Wireless LAN wireless network device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 2 cm between you (or any other person in the vicinity) and the antenna that is built into the computer.

Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If the equipment is not installed and used in accordance with the instructions, the equipment may cause harmful interference to radio communications. There is

no guarantee, however, that such interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

> **NOTE**: The Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations.

U.S. Frequency Bands

2.400 - 2.462 GHz

Canada—Industry Canada (IC)

This Class B digital apparatus complies with Canadian ICES-003, Issue 2, and RSS-210, Issue 4 (Dec. 2000).

Cet appareil numérique de la classe B est conforme à la norme NMB-003, No. 2, et CNR-210, No 4 (Dec 2000).

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing."

« Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé a l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence.»

Europe—EU Declaration of Conformity

European Frequency Bands

2.400 - 2.4835 GHz (Europe ETSI)

Declaration of Conformity

We, **INTEL CORPORATION SA** ; Branch Office; Veldkant 31; 2550 Kontich; Belgium
Declare that the **INTEL® PRO/Wireless 2200BG Network Connection** with model name: **WM3A2200BG**
is in conformance with the essential requirements of the European Council Directive:

1999/5/EC (R&TTE)	Radio and Telecommunications Terminal Equipment Directive (Following Annex IV of this Directive)

is in conformance with the essential requirements of the European Council Directive:

1999/5/EC (R&TTE)	Radio and Telecommunications Terminal Equipment Directive (Following Annex IV of this Directive)

The essential requirements being:

Health & Safety of the user (article 3.1.a)	Following directive 73/23/EEC & European Council Recommendation 1999 519 EC
Electromagnetic Compatibility (article 3.1.b)	Following directive 89/336/EEC
Effective use of the spectrum (article 3.2)	Following the Notified Body Opinion from TNO Certification B.V. with Notified Body number 0336

This declaration is based upon compliance to the following standards:

IEC 60950 (1999 3rd Edition with amendments 1, 2, 3, 4) & EN 60950 (2000)	Safety Information Technology Equipment, Including Electrical Business Equipment. & Common modifications, special national conditions and National Deviation
EN 301 489-1 v1.4.1, Aug. 2002 EN 301 489-17 v1.2.1, Aug. 2002	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services: Part 1: Common technical requirements Part 17: Specific conditions for Wideband Data and Hiperlan equipment
EN 300 328-1 v1.4.1, Apr 2003	Electromagnetic compatibility and Radio Spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques. Part 2: Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
EN 50371	Generic standard to demonstrate the compliance of low power electronic and electrical apparatus with the basis restrictions related to human exposure to electromagnetic fiels (10MHz - 300GHz) - General public

This declaration is made under our sole responsibility.
Authorized Signature by

Date: 01 December 2003

Vincent Colin,
Worldwide Homologations Manager ,
WPD Regulatory Department

intel.

CE0336 ⓘ

Declaration of Conformity

We, **INTEL CORPORATION SA** ; Branch Office; Veldkant 31; 2550 Kontich; Belgium
Declare that the **INTEL® PRO/Wireless 2200BG Network Connection** with model name: **WM3B2200BG** is in conformance with the essential requirements of the European Council Directive:

1999/5/EC (R&TTE)	Radio and Telecommunications Terminal Equipment Directive (Following Annex IV of this Directive)

The essential requirements being:

Health & Safety of the user (article 3.1.a)	Following directive 73/23/EEC & European Council Recommendation 1999 519 EC
Electromagnetic Compatibility (article 3.1.b)	Following directive 89/336/EEC
Effective use of the spectrum (article 3.2)	Following the Notified Body Opinion from TNO Certification B.V. with Notified Body number 0336

This declaration is based upon compliance to the following standards:

IEC 60950 (1999 3rd Edition with amendments 1, 2, 3, 4) & EN 60950 (2000)	Safety Information Technology Equipment, Including Electrical Business Equipment. & Common modifications, special national conditions and National Deviation
EN 301 489-1 v1.4.1, Aug. 2002 EN 301 489-17 v1.2.1, Aug. 2002	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services: Part 1: Common technical requirements Part 17: Specific conditions for Wideband Data and Hiperlan equipment
EN 300 328-1 v1.4.1, Apr 2003	Electromagnetic compatibility and Radio Spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques. Part 2: Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
EN 50371	Generic standard to demonstrate the compliance of low power electronic and electrical apparatus with the basis restrictions related to human exposure to electromagnetic fiels (10MHz - 300GHz) - General public

This declaration is made under our sole responsibility.
Authorized Signature by

Date: 01 December 2003

Vincent Colin,
Worldwide Homologations Manager ,
WPD Regulatory Department

Vincent Colin,
Worldwide Homologations Manager ,
WPD Regulatory Department

This equipment complies with the essential requirements of the European Union directive 1999/5/EC.

English	Hereby, Intel(R) Corporation, declares that this Intel(R) PRO/Wireless 2200BG Network Connection is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Intel(R) Corporation vakuuttaa täten että Intel(R) PRO/Wireless 2200BG Network Connectiontyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) PRO/Wireless 2200BG Network Connection in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
	Bij deze verklaart Intel(R) Corporation dat deze Intel(R) PRO/Wireless 2200BG Network Connection voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) PRO/Wireless 2915ABG Network Connection est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
	Par la présente, Intel(R) Corporation déclare que ce Intel(R) PRO/Wireless 2200BG Network Connection est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
Swedish	Härmed intygar Intel(R) Corporation att denna Intel(R) PRO/Wireless 2200BG Network Connection står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) PRO/Wireless 2200BG Network Connection overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	Hiermit erklärt Intel(R) Corporation, dass sich dieser/diese/dieses Intel(R) PRO/Wireless 2200BG Network Connection in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)
	Hiermit erklärt Intel(R) Corporation die Übereinstimmung des Gerätes Intel(R) PRO/Wireless 2200BG Network Connection mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) PRO/Wireless 2200BG Network Connection ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Icelandic	*Intel* lysir her med yfir að thessi bunadur, Intel(R) PRO/Wireless 2200BG Network Connection, uppfyllir allar grunnkrofur, sem gerdar eru i R&TTE tilskipun ESB nr 1999/5/EC.
Italian	Con la presente Intel(R) Corporation dichiara che questo Intel(R) PRO/Wireless 2200BG Network Connectionè conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente Intel(R) Corporation declara que el Intel(R) PRO/Wireless 2200BG Network Connectioncumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Portuguese	Intel(R) Corporation declara que este Intel(R) PRO/Wireless 2200BG Network Connection está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Malti	Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) PRO/Wireless 2200BG Network Connection jikkonforma mal-•ti•ijiet essenzjali u ma provvedimenti o•rajn relevanti li hemm fid-Dirrettiva 1999/5/EC

New Member States Requirements of Declaration of Conformity

Estonian	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) PRO/Wireless 2200BG Network Connectionvastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

Hungarian	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) PRO/Wireless 2200BG Network Connectionmegfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak
Slovak	Intel(R) Corporation týmto vyhlasuje, že Intel(R) PRO/Wireless 2200BG Network Connection sp••a základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Czech	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) PRO/Wireless 2200BG Network Connection je ve shod• se základními požadavky a dalšími p•íslušnými ustanoveními sm•rnice 1999/5/ES."
Slovenia	Šiuo Intel(R) Corporation deklaruoja, kad šis Intel(R) PRO/Wireless 2200BGNetwork Connectionatitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Latvian	Ar šo Intel(R) Corporation deklar•, ka Intel(R) PRO/Wireless 2200BG Network Connection atbilst Direkt•vas 1999/5/EK b•tiskaj•m pras•b•m un citiem ar to saist•tajiem noteikumiem
Lithuanian	Intel(R) Corporation deklaruoja, kadIntel(R) Pro/Wireless 2200BG Network Connectionatitinka 1999/5/EC Direktyvosesminius reikalavimus irkitas nuostatas".
Polish	Niniejszym, Intel(R) Corporation, deklaruj•, •e Intel(R) PRO/Wireless 2200BG Network Connection spe•nia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.

France

Pour la France métropolitaine
2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
2.400 -2.454 GHz (canaux 1 à 7) autorisé en usage extérieur

Pour la Guyane et la Réunion
2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
2.420 - 2.4835 GHz (canaux 5 à 13) autorisé en usage extérieur

Pour tout le territoire Français:

Seulement 5.15 -5.35 GHz autorisé pour le 802.1

Belgique

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

In geval van privé-gebruik, buiten een gebouw, op een openbare plaats, is geen registratie nodig, wanneer de afstand minder dan 300m is. Voor een afstand groter dan 300m is een registratie bij BIPT vereist. Voor registraties en licenties, gelieve BIPT te contacteren.

Italia

The use of these equipments is regulated by:

- D.L.gs 1.8.2003, n. 259, article 104 (activity subject to general authorization) for outdoor use and article 105 (free use) for indoor use, in both cases for private use.

- D.M. 28.5.03, for supply to public of RLAN access to networks and telecom services.

L'uso degli apparati è regolamentato da:

- D.L.gs 1.8.2003, n. 259, articoli 104 (attività soggette ad autorizzazione generale) se utilizzati al di fuori del proprio fondo e 105 (libero uso) se utilizzati entro il proprio fondo, in entrambi i casi per uso privato.

- D.M. 28.5.03, per la fornitura al pubblico dell'accesso R-LAN alle reti e ai servizi di telecomunicazioni.

Belarus

2.4 GHz OFDM (802.11g) is not allowed at this time.

Korea

당해 무선설비는 운용 중 전파혼신 가능성이 있음

Taiwan

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功
率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並
改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Pakistan

Pakistan Telecommunication Authority (PTA) Approved.

Radio Approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed in the manufacturer's OEM Regulatory Guidance document.

Back to Contents

Back to Contents

Customer Support

Intel support is available online or by telephone. Available services include the most up-to-date product information, installation instructions about specific products, and troubleshooting tips.

Online Support

Technical Support: http://support.intel.com

Network Product Support: http://www.intel.com/network

Corporate Web Site: http://www.intel.com

Back to Contents

Back to Contents

Warranty

Product Warranty Information

One-Year Limited Hardware Warranty

Limited Warranty

In this warranty statement, the term "Product" applies to the following devices:

- Intel(R) WiMAX/WiFi Link 5350
- Intel(R) WiMAX/WiFi Link 5150
- Intel(R) WiFi Link 5300
- Intel(R) WiFi Link 5100
- Intel(R) Wireless WiFi Link 4965AGN
- Intel(R) Wireless WiFi Link 4965AG_
- Intel(R) PRO/Wireless 3945ABG Network Connection
- Intel(R) PRO/Wireless 2915ABG Network Connection
- Intel(R) PRO/Wireless 2200BG Network Connection

Intel warrants to the purchaser of the Product that the Product, if properly used and installed, will be free from defects in material and workmanship and will substantially conform to Intel’s publicly available specifications for the Product for a period of one (1) year beginning on the date the Product was purchased in its original sealed packaging.

SOFTWARE OF ANY KIND DELIVERED WITH OR AS PART OF THE PRODUCT IS EXPRESSLY PROVIDED "AS IS", SPECIFICALLY EXCLUDING ALL OTHER WARRANTIES, EXPRESS, IMPLIED (INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE), provided however, that Intel warrants that the media on which the software is furnished will be free from defects for a period of ninety (90) days from the date of delivery. If such a defect appears within the warranty period, you may return the defective media to Intel for replacement or alternative delivery of the software at Intel's discretion and without charge. Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the software.

If the Product which is the subject of this Limited Warranty fails during the warranty period for reasons covered by this Limited Warranty, Intel, at its option, will:

- **REPAIR** the Product by means of hardware and/or software; OR
- **REPLACE** the Product with another product, OR, if Intel is unable to repair or replace the Product,
- **REFUND** the then-current Intel price for the Product at the time a claim for warranty service is made to Intel under this Limited Warranty.

THIS LIMITED WARRANTY, AND ANY IMPLIED WARRANTIES THAT MAY EXIST UNDER APPLICABLE STATE, NATIONAL, PROVINCIAL OR LOCAL LAW, APPLY ONLY TO YOU AS THE ORIGINAL PURCHASER OF THE PRODUCT.

Extent of Limited Warranty

Intel does not warrant that the Product, whether purchased stand-alone or integrated with other products, including without limitation, semi-conductor components, will be free from design defects or errors known as "errata." Current characterized errata are available upon request. Further, this Limited Warranty does NOT cover: (i) any costs associated with the replacement or repair of the Product, including labor, installation or other costs incurred by you, and in particular, any costs relating to the removal or replacement of any Product soldered or otherwise permanently affixed to any printed circuit board or integrated with other products; (ii) damage to the Product due to external causes, including accident, problems with electrical power, abnormal, mechanical or environmental conditions, usage not in accordance with product instructions, misuse, neglect, accident, abuse, alteration, repair, improper or unauthorized installation or improper testing, or (iii) any Product which has been modified or operated outside of Intel's publicly available specifications or where the original product identification markings (trademark or serial number) have been removed, altered or obliterated from the Product; or (iv) issues resulting from modification (other than by Intel) of software products provided or included in the Product, (v) incorporation of software products, other than those software products provided or included in the Product by Intel, or (vi) failure to apply Intel-supplied modifications or corrections to any software provided with or included in the Product.

How to Obtain Warranty Service

To obtain warranty service for the Product, you may contact your original place of purchase in accordance with its instructions or you may contact Intel. To request warranty service from Intel, you must contact the Intel Customer Support ("ICS") center in your region (www.intel.com/support/) within the warranty period during normal business hours (local time), excluding holidays and return the Product to the designated ICS center. Please be prepared to provide: (1) your name, mailing address, email address, telephone numbers and, in the USA, valid credit card information; (2) proof of purchase; (3) model name and product identification number found on the Product; and (4) an explanation of the problem. The Customer Service Representative may need additional information from you depending on the nature of the problem. Upon ICS's verification that the Product is eligible for warranty service, you will be issued a Return Material Authorization ("RMA") number and provided with instructions for returning the Product to the designated ICS center. When you return the Product to the ICS center, you must include the RMA number on the outside of the package. Intel will not accept any returned Product without an RMA number, or that has an

invalid RMA number, on the package. You must deliver the returned Product to the designated ICS center in the original or equivalent packaging, with shipping charges pre-paid (within the USA), and assume the risk of damage or loss during shipment. Intel may elect to repair or replace the Product with either a new or reconditioned Product or components, as Intel deems appropriate. The repaired or replaced product will be shipped to you at the expense of Intel within a reasonable period of time after receipt of the returned Product by ICS. The returned Product shall become Intel's property on receipt by ICS. The replacement product is warranted under this written warranty and is subject to the same limitations of liability and exclusions for ninety (90) days or the remainder of the original warranty period, whichever is longer. If Intel replaces the Product, the Limited Warranty period for the replacement Product is not extended.

WARRANTY LIMITATIONS AND EXCLUSIONS

THIS WARRANTY REPLACES ALL OTHER WARRANTIES FOR THE PRODUCT AND INTEL DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, COURSE OF DEALING AND USAGE OF TRADE. **Some states (or jurisdictions) do not allow the exclusion of implied warranties so this limitation may not apply to you.** ALL EXPRESS AND IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD. **Some states (or jurisdictions) do not allow limitations on how long an implied warranty lasts, so this limitation may not apply to you.**

LIMITATIONS OF LIABILITY

INTEL'S RESPONSIBILITY UNDER THIS OR ANY OTHER WARRANTY, IMPLIED OR EXPRESS, IS LIMITED TO REPAIR, REPLACEMENT OR REFUND, AS SET FORTH ABOVE. THESE REMEDIES ARE THE SOLE AND EXCLUSIVE REMEDIES FOR ANY BREACH OF WARRANTY. TO THE MAXIMUM EXTENT PERMITTED BY LAW, INTEL IS NOT RESPONSIBLE FOR ANY DIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR UNDER ANY OTHER LEGAL THEORY (INCLUDING WITHOUT LIMITATION, LOST PROFITS, DOWNTIME, LOSS OF GOODWILL, DAMAGE TO OR REPLACEMENT OF EQUIPMENT AND PROPERTY, AND ANY COSTS OF RECOVERING, REPROGRAMMING, OR REPRODUCING ANY PROGRAM OR DATA STORED IN OR USED WITH A SYSTEM CONTAINING THE PRODUCT), EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. **Some states (or jurisdictions) do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.** THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR JURISDICTION. ANY AND ALL DISPUTES ARISING UNDER OR RELATED TO THIS LIMITED WARRANTY SHALL BE ADJUDICATED IN THE FOLLOWING FORUMS AND GOVERNED BY THE FOLLOWING LAWS: FOR THE UNITED STATES OF AMERICA, CANADA, NORTH AMERICA AND SOUTH AMERICA, THE FORUM SHALL BE SANTA CLARA, CALIFORNIA, USA AND THE APPLICABLE LAW SHALL BE THAT OF THE STATE OF DELAWARE. FOR THE ASIA PACIFIC REGION (EXCEPT FOR MAINLAND CHINA), THE FORUM SHALL BE SINGAPORE AND THE APPLICABLE LAW SHALL BE THAT OF SINGAPORE. FOR EUROPE AND THE REST OF THE WORLD, THE FORUM SHALL

BE LONDON AND THE APPLICABLE LAW SHALL BE THAT OF ENGLAND AND WALES IN THE EVENT OF ANY CONFLICT BETWEEN THE ENGLISH LANGUAGE VERSION AND ANY OTHER TRANSLATED VERSION(S)OF THIS LIMITED WARRANTY (WITH THE EXCEPTION OF THE SIMPLIFIED CHINESE VERSION), THE ENGLISH LANGUAGE VERSION SHALL CONTROL.

IMPORTANT! UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS SOLD HEREUNDER ARE NOT DESIGNED, OR INTENDED FOR USE IN ANY MEDICAL, LIFE SAVING OR LIFE SUSTAINING SYSTEMS, TRANSPORTATION SYSTEMS, NUCLEAR SYSTEMS, OR FOR ANY OTHER MISSION CRITICAL APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Back to Top

Back to Contents

Trademarks and Disclaimers

Back to Contents

Glossary of Terms

Term	Definition
802.11	The 802.11 standard refers to a family of specifications developed by the IEEE for wireless LAN technology. The 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
802.11a	The 802.11a standard specifies a maximum data transfer rate of 54 Mbps and an operating frequency of 5 GHz. The 802.11a standard uses the Orthogonal Frequency Division Multiplexing (OFDM) transmission method. Additionally, the 802.11a standard supports 802.11 features such as WEP encryption for security.
802.11b	802.11b is an extension to 802.11 that applies to wireless networks and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. Throughput data rate 5+ Mbps in the 2.4 GHz band.
802.11g	The 802.11g standard specifies a maximum data transfer rate of 54 Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11g networks are also referred to as Wi-Fi* networks.
802.11n	A taskgroup of the IEEE 802.11 committee has defined a new draft specification that provides for increased throughput speeds of up to 540 Mbps. The specification provides for Multiple-Input-Multiple-Output (MIMO) technology, or using multiple receivers and multiple transmitters in both the client and access point, to achieve improved performance. The specification is expected to be approved in the late 2008 timeframe.
802.1X	802.1X is the IEEE Standard for Port-Based Network Access Control. This is used in conjunction with EAP methods to provide access control to wired and wireless networks.
AAA Server	Authentication, Authorization and Accounting Server. A system to control access to computer resources and track user activity.
Access Point (AP)	A device that connects wireless devices to another network. For example, a wireless LAN, Internet modem or others.
Ad Hoc Network	A communication configuration in which every computer has the same capabilities, and any computer can initiate a communication session. Also known as a peer-to-peer network, a device to device network or a computer-to-computer network.

AES-CCMP	Advanced Encryption Standard - Counter CBC-MAC Protocol is the new method for privacy protection of wireless transmissions specified in the IEEE 802.11i standard. AES-CCMP provides a stronger encryption method than TKIP. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in 128-bit blocks. AES-CCMP uses the AES block cipher, but restricts the key length to 128 bits. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC) to provide improved security between the mobile client and the access point.
Authentication	Verifies the identity of a user logging onto a network. Passwords, digital certificates, smart cards and biometrics are used to prove the identity of the client to the network. Passwords and digital certificates are also used to identify the network to the client.
Available network	One of the networks listed under Available networks on the Wireless Networks tab of the Wireless Network Connection Properties (Windows XP environment). Any wireless network that is broadcasting and is within receiving range of the WiFi adapter appears on the list.
BER	Bit Error Rate. The ratio of errors to the total number of bits being sent in a data transmission from one location to another.
Bit Rate	The total number of bits (ones and zeros) per second that a network connection can support. Note that this bit rate will vary, under software control, with different signal path conditions.
Broadcast SSID	Used to allow an access point to respond to clients on a wireless network by sending probes.
BSSID	A unique identifier for each wireless client on a wireless network. The Basic Service Set Identifier (BSSID) is the Ethernet MAC address of each adapter on the network.
CA (Certificate Authority)	A corporate certification authority implemented on a server. In addition, Internet Explorer's certificate can import a certificate from a file. A trusted CA certificate is stored in the root store.
CCX (Cisco Compatible eXtension)	Cisco Compatible Extensions Program ensures that devices used on Cisco wireless LAN infrastructure meet the security, management and roaming requirements.
Certificate	Used for client authentication. A certificate is registered on the authentication server (for example, RADIUS server) and used by the authenticator.
CKIP	Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for encryption in 802.11 media. CKIP uses a key message integrity check and message sequence number to improve 802.11 security in infrastructure mode. CKIP is Cisco's version of TKIP.
Client computer	The computer that gets its Internet connection by sharing either the host computer's connection or the access point's connection.

DSSS	Direct Sequence Spread Spectrum. Technology used in radio transmission. Incompatible with FHSS.
EAP	Short for Extensible Authentication Protocol, EAP sits inside of Point-to-Point Protocol's (PPP) authentication protocol and provides a generalized framework for several different authentication methods. EAP is supposed to head off proprietary authentication systems and let everything from passwords to challenge-response tokens and public-key infrastructure certificates all work smoothly.
EAP-AKA	EAP-AKA (Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement) is an EAP mechanism for authentication and session key distribution, using the Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (USIM). The USIM card is a special smart card used with cellular networks to validate a given user with the network.
EAP-FAST	EAP-FAST, like EAP-TTLS and PEAP, uses tunneling to protect traffic. The main difference is that EAP-FAST does not use certificates to authenticate. Provisioning in EAP-FAST is negotiated solely by the client as the first communication exchange when EAP-FAST is requested from the server. If the client does not have a pre-shared secret Protected Access Credential (PAC), it can request to initiate a provisioning EAP-FAST exchange to dynamically obtain one from the server. EAP-FAST documents two methods to deliver the PAC: manual delivery through an out-of-band secure mechanism, and automatic provisioning. • Manual delivery mechanisms can be any delivery mechanism that the administrator of the network feels is sufficiently secure for their network. • Automatic provisioning establishes an encrypted tunnel to protect the authentication of the client and the delivery of the PAC to the client. This mechanism, while not as secure as a manual method may be, is more secure than the authentication method used in LEAP. The EAP-FAST method can be divided into two parts: provisioning, and authentication. The provisioning phase involves the initial delivery of the PAC to the client. This phase only needs to be performed once per client and user.
EAP-GTC	The EAP-GTC (Generic Token Card) is similar to the EAP-OTP except with hardware token cards. The request contains a displayable message, and the response contains the string read from the hardware token card.
EAP-OTP	EAP-OTP (One-Time Password) is similar to MD5, except it uses the OTP as the response. The request contains a displayable message. The OTP method is defined in RFC 2289.

EAP-SIM	Extensible Authentication Protocol-Subscriber Identity Module (EAP-SIM) authentication can be used with: • Network Authentication types: Open, Shared, and WPA*-Enterprise, WPA2*-Enterprise. • Data Encryption types: None, WEP and CKIP. A SIM card is a special smart card that is used by Global System for Mobile Communications (GSM) based digital cellular networks. The SIM card is used to validate your credentials with the network
EAP-TLS	A type of authentication method that uses EAP and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates that use passwords. EAP-TLS authentication supports dynamic WEP key management.
EAP-TTLS	A type of authentication method that uses EAP and Tunneled Transport Layer Security (TTLS). EAP-TTLS uses a combination of certificates and another security method such as passwords.
Encryption	Scrambling data so that only the authorized recipient can read it. Usually a key is needed to interpret the data.
FHSS	Frequency-Hop Spread Spectrum. Technology used in radio transmission. Incompatible with DSSS.
File and printer sharing	A capability that allows a number of people to view, modify, and print the same file(s) from different computers.
Fragmentation threshold	The threshold at which the wireless adapter breaks the packet into multiple frames. This determines the packet size and affects the throughput of the transmission.
GHz (Gigahertz)	A unit of frequency equal to 1,000,000,000 cycles per second.
Host computer	The computer that is directly connected to the Internet via a modem or network adapter.
Infrastructure network	A wireless network centered around an access point. In this environment, the access point not only provides communication with the wired network, but also mediates wireless network traffic in the immediate neighborhood.
IEEE	Institute of Electrical and Electronics Engineers (IEEE) is an organization involved in defining computing and communications standards.
Internet Protocol (IP) address	The address of a computer that is attached to a network. Part of the address designates which network the computer is on, and the other part represents the host identification.
LAN (Local Area Network)	A high-speed, low-error data network covering a relatively small geographic area.

LEAP (Light Extensible Authentication Protocol)	A version of Extensible Authentication Protocol (EAP). LEAP is a proprietary extensible authentication protocol developed by Cisco that provides a challenge-response authentication mechanism and dynamic key assignment.
MAC (Media Access Control) Address	A hardwired address applied at the factory. It uniquely identifies network hardware, such as a wireless adapter, on a LAN or WAN.
Mbps (Megabits-per-second)	Transmission speed of 1,000,000 bits per second.
MHz (Megahertz)	A unit of frequency equal to 1,000,000 cycles per second.
MIC (Michael)	Message Integrity Check (commonly called Michael).
MS-CHAP	An EAP mechanism used by the client. Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2, is used over an encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel.
ns (Nanosecond)	1 billionth (1/1,000,000,000) of a second.
OFDM	Orthogonal Frequency Division Multiplexing.
Open authentication	Allows any device network access. If encryption is not enabled on the network, any device that knows the Service Set Identifier (SSID) of the access point can gain access to the network.
PEAP	Protected Extensible Authentication Protocol (PEAP) is an Internet Engineering Task Force (IETF) draft protocol sponsored by Microsoft, Cisco, and RSA Security. PEAP creates an encrypted tunnel similar to the tunnel used in secure web pages (SSL). Inside the encrypted tunnel, a number of other EAP authentication methods can be used to perform client authentication. PEAP requires a TLS certificate on the RADIUS server, but unlike EAP-TLS there is no requirement to have a certificate on the client. PEAP has not been ratified by the IETF. The IETF is currently comparing PEAP and TTLS (Tunneled TLS) to determine an authentication standard for 802.1X authentication in 802.11 wireless systems. PEAP is an authentication type designed to take advantage of server-side EAP-Transport Layer Security (EAP-TLS) and to support various authentication methods, including user passwords and one-time passwords, and Generic Token Cards.
Peer-to-Peer mode	A wireless network structure that allows wireless clients to communicate directly with each other without using an access point.
Power save mode	The state in which the radio is periodically powered down to conserve power. When the portable computer is in Power Save mode, received packets are stored in the access point until the wireless adapter wakes up.

Preferred network	One of the networks that has been configured. Such networks are listed under Preferred networks on the Wireless Networks tab of the Wireless Network Connection Properties (Windows XP* environment).
RADIUS (Remote Authentication Dial-In User Service)	RADIUS is an authentication and accounting system that verifies user's credentials and grants access to requested resources.
RF (Radio Frequency)	The international unit for measuring frequency is Hertz (Hz), which is equivalent to the older unit of cycles per second. One MegaHertz (MHz) is one million Hertz. One GigaHertz (GHz) is one billion Hertz. For reference: the standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55 -1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and microwave ovens typically operate at 2.45 GHz.
Roaming	Movement of a wireless node between two micro cells. Roaming usually occurs in infrastructure networks built around multiple access points. Current wireless network roaming is only supported in the same subnet of a network.
RTS threshold	The number of frames in the data packet at or above which an RTS/CTS (request to send/clear to send) handshake is turned on before the packet is sent. The default value is 2347.
Shared key	An encryption key known only to the receiver and sender of data. This is also referred to as a pre-shared key.
SIM (Subscriber Identity Module)	A SIM card is used to validate credentials with the network. A SIM card is a special smart card used by GSM-based digital cellular networks.
Silent mode	Silent Mode Access Points or Wireless Routers have been configured to not broadcast the SSID for the wireless network. This makes it necessary to know the SSID in order to configure the wireless profile to connect to the access point or wireless router.
Single Sign On	Single Sign On feature set allows the 802.1X credentials to match your Windows log on user name and password credentials for wireless network connections.
SSID (Service Set Identifier)	SSID or network name is a value that controls access to a wireless network. The SSID for your wireless network card must match the SSID for any access point that you want to connect with. If the value does not match, you are not granted access to the network. Each SSID may be up to 32 alphanumeric characters long and is case-sensitive.

stealth	A stealth access point is one that has the capability and is configured to not broadcast its SSID. This is the WiFi network name that appears when a DMU (Device Management Utility, such as Intel® PROSet/Wireless WiFi) scans for available wireless networks. Although this can enhance wireless network security, it is commonly considered a weak security feature. To connect to a stealth access point, a user must specifically know the SSID and configure their DMU accordingly. The feature is not a part of the 802.11 specification, and is known by differing names by various vendors: closed mode, private network, SSID broadcasting.
TKIP (Temporal Key Integrity Protocol)	Temporal Key Integrity protocol improves data encryption. Wi-Fi Protected Access* uses its TKIP. TKIP provides important data encryption enhancements including a re-keying method. TKIP is part of the IEEE 802.11i encryption standard for wireless networks. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless networks. TKIP provides per packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.
TLS (Transport Layer Security)	A type of authentication method using the Extensible Authentication Protocol (EAP) and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates which use passwords. EAP-TLS authentication supports dynamic WEP key management. The TLS protocol is intended to secure and authenticate communications across a public network through data encryption. The TLS Handshake Protocol allows the server and client to provide mutual authentication and to negotiate an encryption algorithm and cryptographic keys before data is transmitted.
TTLS (Tunneled Transport Layer Security)	These settings define the protocol and the credentials used to authenticate a user. In TTLS, the client uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client can use another authentication protocol. Typically password-based protocols challenge over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel. TTLS implementations today support all methods defined by EAP, as well as several older methods (CHAP, PAP, MS-CHAP and MS-CHAP-V2). TTLS can easily be extended to work with new protocols by defining new attributes to support new protocols.
WEP (Wired Equivalent Privacy)	Wired Equivalent Privacy, 64- and 128-bit (64-bit is sometimes referred to as 40-bit). This is a low-level encryption technique designed to give the user about the same amount of privacy that he would expect from a LAN. WEP is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by data over radio waves so that it is protected as it is transmitted from one end point to another.

<table>
<tr><td>WEP Key</td><td>Either a pass phrase or hexadecimal key.
The pass phrase must be 5 ASCII characters for 64-bit WEP or 13 ASCII characters for 128-bit WEP. For pass phrases, 0-9, a-z, A-Z, and ~!@#$% ^&*()_+|`-={}|[]\:";'<>?,./ are all valid characters.
The hex key must be 10 hexadecimal characters (0-9, A-F) for 64-bit WEP or 26 hexadecimal characters (0-9, A-F) for 128-bit WEP.</td></tr>
<tr><td>Wi-Fi* (Wireless Fidelity)</td><td>Is meant to be used generically when referring of any type to 802.11 network, whether 802.11b, 802.11a, or dual-band.</td></tr>
<tr><td>WiMAX</td><td>WiMAX, the Worldwide Interoperability for Microwave Access, is a telecommunications technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access. It is based on the IEEE 802.16 standard. The name WiMAX was created by the WiMAX Forum, which was formed in June 2001 to promote conformance and interoperability of the standard. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL."</td></tr>
<tr><td>Wireless router</td><td>A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer within the same network and to connect to the Internet.</td></tr>
<tr><td>WLAN (Wireless Local-Area Network)</td><td>A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.</td></tr>
<tr><td>WPA* (Wi-Fi Protected Access)</td><td>This is a security enhancement that strongly increases the level of data protection and access control to a wireless network. WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion. WPA consists of RC4 and TKIP and provides support for BSS (Infrastructure) mode only. WPA and WPA2 are compatible.</td></tr>
<tr><td>WPA2* (Wi-Fi Protected Access 2)</td><td>This is the second generation of WPA that complies with the IEEE TGi specification. WPA2 consists of AES encryption, pre-authentication and PMKID caching. It provides support for BSS (Infrastructure) mode and IBSS (ad hoc) mode. WPA and WPA2 are compatible.</td></tr>
</table>

WPA-Enterprise	Wi-Fi Protected Access-Enterprise applies to corporate users. A new standards-based, interoperable security technology for wireless LAN (subset of IEEE 802.11i draft standard) that encrypts data sent over radio waves. WPA is a Wi-Fi standard that was designed to improve upon the security features of WEP as follows: • Improved data encryption through the temporal key integrity protocol (TKIP). TKIP uses a hashing algorithm to scramble the encryption keys and adds an integrity-checking feature to ensure that the keys have not been tampered with. • User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network. WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion.
WPA-Personal	Wi-Fi Protected Access-Personal provides a level of security in the small network or home environment.
WPA-PSK (Wi-Fi Protected Access-Pre-Shared Key)	WPA-PSK mode does not use an authentication server. It can be used with the data encryption types WEP or TKIP. WPA-PSK requires configuration of a pre-shared key (PSK). You must enter a pass phrase or 64 hex characters for a pre-shared key of length 256-bits. The data encryption key is derived from the PSK.

Back to Top

Back to Contents